Центральный изолятор Symantec™ Руководство администратора



Центральный изолятор Symantec™ Руководство администратора

Программное обеспечение, описанное в этой книге, поставляется вместе с лицензионным соглашением и может использоваться только при соблюдении условий этого соглашения.

Версия документации: 8.0

Авторские права

Товарные знаки

Напечатано в Ирландии.

10 9 8 7 6 5 4 3 2 1

Оглавление

Глава 4 Работа в режиме осмотра и доставки через Интернет

Приложение A Справка по обработке образцов

Глава 1

Изолятор – Введение

Эта глава содержит следующие разделы:

О программе Изолятор

Когда продукт Symantec или Symantec AntiVirus обнаруживает зараженный объект, который нельзя исправить с помощью текущего набора описаний вирусов, он блокирует доступ к этому объекту и помещает его в локальный Изолятор – специальное хранилище для файлов, зараженных вирусами. Вирусы, находящиеся в локальном Изоляторе, не могут распространиться по другим областям зараженного компьютера.

Продукт Symantec или Symantec AntiVirus может автоматически пересылать зараженные файлы из локального Изолятора в Центральный изолятор, представляющий собой централизованное хранилище зараженных файлов, если соответствующая функция настроена. Центральный изолятор состоит из двух компонентов: сервера Изолятора и консоли Изолятора, модуля Microsoft Management Console (MMC). В Центральном изоляторе можно настроить один из двух способов осмотра и доставки зараженных файлов:

- Осмотр и доставка через Интернет: Полностью автоматизированная система передачи зараженных файлов в центр Symantec Security Response (ранее известный как Symantec AntiVirus Research Center, или SARC) для их анализа и исправления.
- Осмотр и доставка по электронной почте: Полуавтоматическая система, требующая участия администратора в процедуре отправки зараженных файлов и доставки описаний вирусов.

В обоих вариантах осмотра и доставки используется система Digital Immune System компании Symantec.

Сведения о Digital Immune System

Антивирусные программы предыдущего поколения были предназначены для защиты рабочих станций от вирусов. В конце 1990-х годов такие печально известные вирусы, как Melissa, наглядно продемонстрировали, что одной защиты рабочих станций недостаточно. Хотя многие рабочие станции и серверы, пораженные вирусом Melissa, были защищены самым современным антивирусным программным обеспечением, они не смогли противостоять атаке вируса.

При разработке продукта Digital Immune System компания Symantec постаралась снять ограничения, которые существовали в других антивирусных программах. Digital Immune System – это полностью автоматизированная антивирусная система замкнутого цикла. Она контролирует весь процесс борьбы с вирусами, в том числе обнаружение

вирусов, анализ вирусов и рассылку исправлений на пораженные компьютеры. Кроме того, Digital Immune System позволяет автоматизировать выполнение множества задач, связанных с обнаружением, отправкой и анализом вирусов и рассылкой исправлений. Автоматизация значительно сокращает интервал времени между обнаружением вируса и распространением исправления, что повышает эффективность мер по борьбе с вирусами.

Digital Immune System выполняет следующие задачи:

- Идентифицирует и изолирует: Оперативно обнаруживает новые вирусы, используя мощные методы эвристического и бихевиористического анализа. Подозрительные объекты помещаются в Центральный изолятор, а образцы автоматически отправляются в центр Symantec Security Response для анализа.
- Анализирует: Отправляет файлы в Symantec Security Response для анализа, исправления и проверки.
- Исправляет: Автоматически доставляет исправления на серверы клиентов.

Обнаружение и изоляция вирусов

Одна из основных задач Digital Immune System состоит в обнаружении новых или неизвестных вирусов на рабочих станциях, серверах и шлюзе. Для этой цели компания Symantec применяет эвристическую технологию Bloodhound™, позволяющую обнаруживать большинство новых или неизвестных вирусов.

Клиенты автоматически отправляют подозрительные файлы в локальный Изолятор, расположенный на рабочей станции, сервере или шлюзе, если включена соответствующая функция. В локальном Изоляторе подозрительные файлы упаковываются вместе с информацией о передавшем их компьютере и пересылаются в корпоративный Центральный изолятор для дальнейшего анализа.

Поскольку Центральный изолятор обычно располагает большим числом описаний вирусов по сравнению с исходным компьютером, он еще раз просматривает файлы, используя собственный набор описаний вирусов. Если Центральный изолятор в состоянии исправить файл, он отправляет свежие описания вирусов на зараженный компьютер. Если Центральный изолятор не может исправить файл, он удаляет из него данные, которые могут носить конфиденциальный характер (например, из файлов Microsoft Word удаляется текст), и зашифровывает файл. После этого Digital Immune

System передает файл через Интернет на шлюз Symantec для дальнейшего анализа.

Администратор может настроить Digital Immune System для автоматического выполнения следующих задач:

- Обнаружение и изоляция новых и неизвестных вирусов.
- Фильтрация и пересылка зашифрованных образцов в Symantec Security Response для анализа (с предварительным удалением конфиденциальной информации, если это необходимо).
- Проверка наличия новых описаний вирусов и обновлений.
- Распространение новых описаний среди зараженных компьютеров или среди более широкого круга компьютеров.

См. «Компоненты Digital Immune System и Центрального изолятора» на стр. 11.

См. «Включение и настройка Центрального изолятора, работающего через Интернет» на стр. 32.

Анализ вирусов

Агент Изолятора управляет обменом данными между Центральным изолятором и шлюзом Symantec. Если Центральному изолятору не удалось исправить зараженный файл, агент Изолятора пересылает этот файл на шлюз. После этого агент Изолятора отправляет запрос на шлюз, чтобы узнать, было ли создано исправление.

- Если да, агент Изолятора загружает новый набор описаний вирусов и устанавливает его в Центральном изоляторе. Затем агент Изолятора проверяет, нужно ли установить обновленные описания на исходном компьютере, и, при необходимости, отправляет эти описания.
- Если исправление еще не создано, агент Изолятора опрашивает шлюз каждые 60 минут.

Когда система Digital Immune System получает новую информацию, она выполняет следующие действия:

- Добавляет полученную информацию в учетную базу данных.
- Фильтрует полученную информацию, исключая из нее незараженные файлы, ложно обнаруженные вирусы и известные вирусы. Фильтрация выполняется быстро. Поскольку большая часть данных отфильтровывается, время ответа для отфильтрованных элементов крайне невелико.

- Анализирует вирус, создает исправление и тестирует его. В большинстве случаев анализ вируса и создание исправления выполняется автоматически, однако иногда может потребоваться вмешательство исследователей из центра Symantec Security Response.
- Создает новый набор описаний вирусов, включающий описание нового вируса, и возвращает эти описания шлюзу.

Исправление зараженных файлов

Когда в ходе опроса шлюза агент Изолятора получает уведомление о том, что исправление готово, он загружает набор описаний вирусов и устанавливает его в Центральном изоляторе. Затем агент Изолятора проверяет, нужно ли установить обновленный набор описаний на исходном компьютере, и, при необходимости, передает этот набор описаний.

Компоненты Digital Immune System и Центрального изолятора

Компоненты Digital Immune System и Центрального изолятора Symantec перечислены в Табл. 1-1.

Табл. 1-1 Компоненты Digital Immune System и Центрального изолятора

Компонент	Описание
Symantec Security Response	Автоматизированный центр анализа, который на основе полученных образцов создает и распространяет обновленные описания вирусов.
Шлюз	Промежуточный узел, расположенный между Symantec Security Response и Центральным изолятором. Шлюз анализирует образцы и пересылает их в Symantec Security Response лишь в том случае, если ему не удалось исправить образцы с помощью собственного набора описаний вирусов. Если образец удалось исправить, шлюз возвращает описания вирусов Центральному изолятору.

Табл. 1-1 Компоненты Digital Immune System и Центрального изолятора

Компонент	Описание
Консоль Изолятора	Пользовательский интерфейс для работы с Центральным изолятором, предназначенный для настройки Центрального изолятора, обмена данными со шлюзом и управления обновлением описаний.
Сервер Изолятора	Этот компонент принимает зараженные файлы от серверов и клиентов и обменивается данными с Центральным изолятором. Объекты, поступающие в Изолятор, вначале проверяются с помощью набора описаний сервера Изолятора, и передаются далее, если их не удалось исправить. Сервер Изолятора настроен для приема данных через порты протоколов IP и SPX. Клиент должен быть настроен для передачи данных через порт, соответствующий тому протоколу, который используется на клиенте.
Агент Изолятора	Этот компонент управляет обменом данными между сервером Изолятора и шлюзом, а также активизирует механизм Defcast. Кроме того, агент Изолятора следит за тем, чтобы в Центральном изоляторе был установлен самый свежий набор описаний из тех, что присутствуют на шлюзе.
Сканер Изолятора	Компонент, который осматривает переданные файлы с помощью набора описаний сервера Изолятора. Перед отправкой образцов из Центрального изолятора их необходимо проверить. Набор описаний, загруженный агентом и применяемый сканером Изолятора, не совпадает с наборами описаний вирусов, которые применяются другими продуктами Symantec AntiVirus на компьютере сервера Изолятора.
Defcast	Этот компонент запрашивает у серверов и клиентов порядковый номер описаний вирусов и, при необходимости, отправляет новый набор описаний.

Табл. 1-1 Компоненты Digital Immune System и Центрального изолятора

Компонент	Описание
Alert Management System (AMS)	Сервер Изолятора может использовать возможности сервера AMS, если он установлен. На сервере Изолятора предусмотрен свой набор событий и оповещений AMS, а также свой журнал AMS.

См. «Настройка оповещений» на стр. 53.

См. «Сведения о Digital Immune System» на стр. 8.

См. «Включение и настройка Центрального изолятора, работающего через Интернет» на стр. 32.

Работа в режиме осмотра и доставки через Интернет

В режиме осмотра и доставки через Интернет сервер Центрального изолятора можно настроить для автоматической передачи образцов зараженных объектов в центр Symantec Security Response для их анализа и исправления без вмешательства администратора. Когда Symantec Security Response получает зараженный объект через Интернет, он анализирует полученную информацию и возвращает обновленные описания вирусов соответствующему компьютеру клиента через Интернет. Новые описания автоматически устанавливаются на сервере Изолятора, а также, в зависимости от конфигурации, на шлюзе, сервере и рабочей станции, отправившей зараженный файл.

Работа в режиме осмотра и доставки по электронной почте

Если включен режим осмотра и доставки по электронной почте, администратор вручную отправляет подозрительные файлы в центр Symantec Security Response по электронной почте для их анализа и исправления. Для упрощения этой процедуры на консоли Изолятора предусмотрен мастер осмотра и доставки. Symantec Security Response анализирует полученную информацию, а затем отправляет администратору зараженного компьютера ответное письмо, содержащее исправление в виде новых файлов описаний вирусов.

См. «Работа в режиме осмотра и доставки по электронной почте» на стр. 21.

Выбор режима осмотра и доставки

Режим осмотра и доставки выбирается во время установки.

- Выберите режим осмотра и доставки по электронной почте, если вы хотите вручную отправлять образцы вирусов в центр Symantec Security Response, а затем вручную применять новые описания вирусов на компьютерах сети.
- Выберите режим осмотра и доставки через Интернет, если сервер Изолятора должен автоматически отправлять описания вирусов в центр Symantec Security Response, а затем автоматически применять новые описания вирусов на компьютерах сети.

Сведения о центре Symantec Security Response

В центре Symantec Security Response команда квалифицированных специалистов в области компьютерных вирусов круглосуточно работает над созданием технологии обнаружения и уничтожения вирусов. Существенную помощь в этом оказывает система Symantec AntiVirus Research Automation (SARA). SARA автоматически анализирует значительную часть полученных образцов вирусов. Соответствующие описания вирусов автоматически создаются и оперативно рассылаются клиентам, что позволяет быстро остановить распространение новых вирусов.

Глава 2

Установка и настройка Центрального изолятора

Эта глава содержит следующие разделы:

Подготовка к установке

Перед установкой Центрального изолятора ознакомьтесь со следующей информацией:

- Для установки консоли и сервера Изолятора необходимы права администратора. Перед началом установки убедитесь, что у вас есть необходимые права.
- В состав Центрального изолятора входят сервер Изолятора и консоль Изолятора. Сервер Изолятора и консоль Изолятора можно установить на один компьютер Windows NT/2000 или на разные компьютеры.
- На консоли Изолятора должен применяться тот же сетевой протокол (TCP/IP или IPX/SPX), что и на сервере Изолятора. В противном случае с ее помощью нельзя будет настроить сервер.
- Продукты, поддерживающие Изолятор, могут пересылать файлы серверу Изолятора по протоколу TCP/IP или IPX/SPX, поэтому на сервере Изолятора должны быть установлены оба указанных протокола.
- Если вы планируете применять режим осмотра и доставки через Интернет, убедитесь, что сервер Изолятора подключен к сети Интернет. Это необходимо для автоматической отправки образцов вирусов и обновления описаний вирусов. Кроме того, убедитесь, что на брандмауэре или прокси-сервере HTTP серверу Изолятора разрешено подключаться к Интернету.

Требования к системе, предъявляемые сервером и консолью Центрального изолятора

- Windows 2000/NT Server 4.0 с пакетом обновления 5 или более поздним
- Модуль Windows NT Server DCOM (только для Windows NT Server 4.0)
- Internet Explorer версии 5.5 с пакетом обслуживания 2 и поддержкой 128-разрядного шифрования или более поздняя версия
- 128 Мб оперативной памяти
- Минимальный размер файла подкачки - 250 Мб
- 15 Мб свободного дискового пространства
- До 4 Гб свободного дискового пространства для изолированных объектов
- Права администратора сервера Windows NT или домена Windows NT

Установка Центрального изолятора

Установка Центрального изолятора включает в себя следующие задачи:

- Установка консоли Изолятора
- Установка сервера Изолятора

Примечание: Если в продукте Symantec предусмотрена возможность автоматической установки консоли и сервера Изолятора, то описанные ниже действия выполнять не нужно.

Для установки Центрального изолятора выполните следующие действия:

Установка Центрального изолятора включает в себя установку консоли Изолятора и сервера Изолятора.

Для установки консоли Изолятора выполните следующие действия:

1 В окне диалога «Установка Symantec Client Security» выберите **Установить средства администрирования SAV.**

2 Выберите **Установить консоль Центрального изолятора.**

3 В окне приветствия нажмите кнопку **Далее.**

4 В окне с лицензионным соглашением нажмите кнопку **Да.**

5 В окне «Выбор каталога для установки» нажмите одну из следующих кнопок:

- Далее: Для установки продукта в папку по умолчанию.
- Обзор: Для выбора другой папки.
  Не устанавливайте консоль Изолятора на сетевой диск.

6 Для завершения установки выполните инструкции, показанные на экране.

Для установки сервера Изолятора выполните следующие действия:

1 В окне диалога «Установка Symantec Client Security» выберите **Установить средства администрирования SAV.**

2 Выберите **Установить сервер Центрального изолятора.**

3 В окне приветствия нажмите кнопку **Далее.**

4 В окне «Выбор каталога для установки» нажмите одну из следующих кнопок:

- Далее: Для установки продукта в папку по умолчанию.
- Обзор: Для выбора другой папки.
  Не устанавливайте сервер Изолятора на сетевой диск.

5 В окне «Тип установки» выберите один из следующих вариантов:

- Интернет (рекомендуется)
  См. «Работа в режиме осмотра и доставки через Интернет» на стр. 31.
- Электронная почта
  См. «Работа в режиме осмотра и доставки по электронной почте» на стр. 21.

6 Нажмите кнопку **Далее.**

7 В окне «Дисковое пространство» оставьте размер дискового пространства по умолчанию, равный 500 Мб, либо введите другое значение в поле «Дисковое пространство (Мб)», а затем нажмите кнопку **Далее**.

8 В окне «Сведения о клиенте» введите название своей организации, учетный номер (если он есть), имя ответственного лица, контактный телефон и адрес электронной почты.

  Заполните все поля и нажмите кнопку **Далее**.

9 В окне «Связь через Интернет» оставьте адрес шлюза по умолчанию или введите другой адрес (если он был предоставлен компанией Symantec), а затем нажмите кнопку **Далее**.

10 В окне «Настройка оповещений» установите флажок **Включить отправку оповещений** и введите имя сервера AMS, если вы планируете применять Alert Management Server (AMS). Нажмите кнопку **Далее**.

11 Для завершения установки выполните инструкции, показанные на экране.

Настройка Центрального изолятора

На основании информации, заданной во время установки, параметрам Центрального изолятора присваиваются значения по умолчанию, которые сами по себе обеспечивают адекватный уровень защиты. Изменять значения параметров не требуется.

См. «Свойства Центрального изолятора» на стр. 35.

См. «Настройка пересылки файлов по электронной почте на клиентах» на стр. 24.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

См. «Настройка оповещений» на стр. 53.

Глава 3

Работа в режиме осмотра и доставки по электронной почте

Эта глава содержит следующие разделы:

- Сведения о режиме осмотра и доставки по электронной почте
- Включение и настройка Центрального изолятора, использующего электронную почту
- Работа с изолированными файлами

Сведения о режиме осмотра и доставки по электронной почте

В этом режиме осмотра и доставки электронная почта применяется для решения следующих задач:

- Передачи образцов в центр Symantec Security Response с помощью мастера осмотра и доставки.
- Получения новых описаний вирусов в случае обнаружения нового вируса.

Включение и настройка Центрального изолятора, использующего электронную почту

В состав Центрального изолятора входят два компонента: сервер Изолятора, который можно установить на любом компьютере Windows NT/2000 для хранения образцов зараженных файлов и обмена данными с центром Symantec Security Response, и консоли Изолятора, которая представляет собой модуль MMC и применяется для управления работой.

Для того чтобы начать использование Центрального изолятора, выполните следующие действия:

- Подключитесь к серверу Изолятора.
- Настройте сервер Изолятора.
- Настройте клиенты для пересылки файлов на сервер Изолятора.
- Настройте функцию «Осмотр и доставка» для передачи образцов в центр Symantec Security Response и получения обновленных описаний.

Примечание: Режим осмотра и доставки через Интернет или по электронной почте выбирается во время установки сервера Изолятора. Для изменения режима необходимо заново установить сервер Изолятора.

См. «Подключение к серверу Изолятора» на стр. 23.

См. «Настройка сервера Изолятора» на стр. 24.

См. «Настройка пересылки файлов по электронной почте на клиентах» на стр. 24.

Подключение к серверу Изолятора

Сервер Изолятора настраивается в качестве центрального хранилища зараженных файлов, которые не удалось исправить на компьютерах-клиентах. После этого можно настроить клиенты на отправку копий файлов, хранящихся в их локальных Изоляторах.

См. «Настройка пересылки файлов по электронной почте на клиентах» на стр. 24.

Для подключения к серверу Изолятора выполните следующие действия:

Можно подключиться к серверу Изолятора, расположенному на локальном компьютере, либо другом компьютере.

Для подключения к серверу Изолятора, расположенному на локальном компьютере, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec**, а затем выберите **Подключение к серверу.**
2. В окне диалога «Подключение к серверу Изолятора» введите имя сервера и нажмите кнопку **OK**.

Для подключения к серверу Изолятора, расположенному на другом компьютере, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Подключение к серверу.**
2. В окне диалога «Подключение к серверу Изолятора» введите имя сервера.
3. Введите имя пользователя и пароль для входа на сервер.
4. Если компьютер является частью домена, введите имя домена.

См. «Настройка сервера Изолятора» на стр. 24.

См. «Настройка пересылки файлов по электронной почте на клиентах» на стр. 24.

Настройка сервера Изолятора

Сервер Изолятора настраивается в качестве центрального хранилища зараженных файлов, которые не удалось исправить на компьютерах-клиентах. В режиме осмотра и доставки по электронной почте для работы с сервером Изолятора требуются следующие сведения:

- Путь к папке, применяемой для хранения файлов на сервере Изолятора
- Протоколы, применяемые в сети, и порты, через которые передаются данные

После этого можно настроить клиенты на отправку копий файлов, хранящихся в их локальных Изоляторах.

См. «Настройка пересылки файлов по электронной почте на клиентах» на стр. 24.

Для настройки сервера Изолятора выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите **Свойства**.
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Общие» и введите полное имя папки Изолятора.
3. Укажите максимальный размер папки Изолятора.
4. Выберите протоколы, используемые в сети, и укажите порт, через который передаются данные.

   Не используйте порт, зарезервированный другим приложением. Как правило, порты с номерами больше 1025 свободны.

См. «Подключение к серверу Изолятора» на стр. 23.

Настройка пересылки файлов по электронной почте на клиентах

Два типа клиентов Центрального изолятора могут пересылать образцы вирусов на сервер Изолятора:

- Управляемые, например, клиенты и серверы Symantec AntiVirus Corporate Edition, управляемые программой Symantec System Center
- Автономные, например, Symantec AntiVirus для Microsoft Exchange и Symantec AntiVirus для Lotus Notes

Основным различием между этими клиентами является способ доставки новых описаний вирусов. В случае доставки по электронной почте, обновленные описания присылаются для всех указанных платформ, и их применением управляет администратор.

В случае доставки через Интернет, обновленные описания доставляются и устанавливаются автоматически только на те компьютеры, которые используют один из управляемых программных продуктов. Для неуправляемых продуктов обновленные описания загружаются и устанавливаются администраторами после получения уведомления.

См. «Управляемые и автономные продукты» на стр. 45.

Для настройки пересылки образцов с клиентов выполните следующие действия:

Пересылку файлов на сервер Изолятора можно настроить на управляемых и автономных клиентах.

Для того чтобы настроить управляемые клиенты для пересылки образцов на сервер Изолятора, выполните следующие действия:

1. На левой панели консоли Symantec System Center щелкните правой кнопкой мыши на группе клиентов, группе серверов или отдельном сервере и выберите **Все задачи** > **Symantec AntiVirus** > **Параметры Изолятора**.
2. В окне диалога «Параметры изолятора» выберите **Включить Изолятор или мастер осмотра и отправки**.
3. Выберите параметр **Разрешить пересылку на сервер Изолятора**.

   Если пересылка включена, то клиенты не могут отправлять файлы напрямую в центр Symantec Security Response из своих Изоляторов.
4. В поле «Имя сервера» введите имя, IP-адрес или SPX-адрес сервера Изолятора.
5. Укажите порт и протокол, заданные при настройке свойств сервера Изолятора.
6. Выберите операцию, которая должна автоматически выполняться в Изоляторе клиента при появлении новых описаний вирусов.

Для того чтобы настроить автономные клиенты для пересылки файлов на сервер Изолятора, выполните следующие действия:

1. Откройте окно настройки параметров пересылки в Изолятор.

   Обратитесь к документации или к справочной системе конкретной программы.
2. Введите имя или IP-адрес компьютера, на котором работает сервер Изолятора.
3. Укажите порт и протокол, заданные при настройке свойств сервера Изолятора.

См. «Подключение к серверу Изолятора» на стр. 23.

См. «Настройка сервера Изолятора» на стр. 24.

Передача файлов для анализа

В состав Изолятора входит мастер осмотра и отправки, упрощающий задачу отправки файлов в центр Symantec Security Response для анализа. Для соблюдения конфиденциальности из файлов, отправляемых в Symantec Security Response, можно удалить личные данные.

Новые описания, полученные по электронной почте, сначала можно применить только в Центральном изоляторе, чтобы проверить их работоспособность. После этого можно переслать обновление на компьютер-клиент (где исходный зараженный файл по-прежнему хранится в Изоляторе), чтобы там было выполнено заранее выбранное действие, например, автоматическое исправление зараженного файла и его извлечение из Изолятора.

См. «Работа с изолированными файлами» на стр. 27.

Отправка файлов в центр Symantec Security Response

Мастер осмотра и отправки упрощает задачу отправки файлов в центр Symantec Security Response для анализа. Этот мастер быстро извлечет зараженную часть файла (исключив личные данные) и отправит ее по электронной почте в Symantec для анализа и оперативного создания описания вируса.

После нажатия кнопки «Отправить» мастер осмотра и отправки проанализирует файл и, при необходимости, порекомендует выполнить другое действие вместо отправки. Например, это может произойти в том случае, если вирус можно уничтожить с помощью текущего набора

описаний. Вы можете отказаться от предложенного действия и отправить образец.

Примечание: Для отправки файлов в центр Symantec Security Response должно быть установлено соединение с Интернетом и задан адрес электронной почты.

Для отправки файла в Symantec Security Response выполните следующие действия:

1 На правой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на имени файла и выберите пункт **Отправить в SARC**.

2 Выполните инструкции мастера осмотра и отправки для сбора необходимой информации и отправки файла в центр Symantec Security Response для анализа.

3 В программе мастера предусмотрено два параметра, применяемых в особых случаях:

   - Обрезать содержимое файла: Если этот параметр выбран, то в центр Symantec Security Response отправляется только та часть файла, которая может быть заражена вирусом. Все конфиденциальные данные и текст удаляются из документа перед отправкой. Тем не менее, в Изоляторе остается полная копия файла.
   - Указать сервер SMTP: Этот параметр применяется в корпоративных системах для отправки файлов из Изолятора в центр Symantec Security Response через собственный сервер SMTP.

Работа с изолированными файлами

По умолчанию клиенты Symantec и Symantec AntiVirus изолируют зараженные объекты, которые нельзя исправить с помощью текущего набора описаний вирусов. Клиенты, которые были настроены на пересылку зараженных файлов, автоматически отправляют копии зараженных объектов на сервер Центрального изолятора.

После помещения файлов в Центральный изолятор можно выполнить следующие действия:

- Просмотреть список изолированных файлов
- Исправить файлы
- Восстановить файлы
- Удалить файлы

См. «Передача файлов для анализа» на стр. 26.

См. «Просмотр списка изолированных объектов» на стр. 28.

См. «Удаление изолированных файлов» на стр. 29.

См. «Исправление и восстановление изолированных файлов» на стр. 30.

Просмотр списка изолированных объектов

Содержимое Центрального изолятора пополняется в том случае, если компьютеры-клиенты настроены на пересылку зараженных объектов в Центральный изолятор. В Табл. 3-1 приведена сохраняемая информация об изолированном файле.

Табл. 3-1 Информация об изолированном файле

Информация о файле	Описание
Имя файла	Имя зараженного объекта
Имя пользователя	Имя владельца зараженного файла
Компьютер	Компьютер, на котором был обнаружен зараженный объект
Имя домена	Домен, в который входит зараженный компьютер
Получен	Время помещения объекта в Изолятор
Отправлен	Время отправки объекта в Symantec Security Response
Отправитель	Имя пользователя, отправившего образец для анализа
Состояние	Состояние обработки образца
Вирус	Название обнаруженного вируса

Для того чтобы просмотреть список изолированных объектов, выполните следующие действия:

Вы можете просмотреть список изолированных объектов и подробную информацию о каждом объекте.

Для просмотра списка изолированных объектов выполните следующие действия:

- На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.

Для получения подробных сведений об изолированном объекте, выполните следующие действия:

1 На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.

2 На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.

См. «Передача файлов для анализа» на стр. 26.

См. «Удаление изолированных файлов» на стр. 29.

См. «Исправление и восстановление изолированных файлов» на стр. 30.

Удаление изолированных файлов

Хотя из Центрального изолятора можно удалять любые объекты, рекомендуется использовать эту возможность только для удаления файлов, которые больше не нужны. После того как с помощью обновленных описаний вирус был обнаружен и уничтожен, изолированный объект можно удалить.

Для удаления изолированных файлов выполните следующие действия:

1 На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.

2 На правой панели щелкните правой кнопкой мыши на одном или нескольких файлах и выберите пункт **Удалить**.

См. «Передача файлов для анализа» на стр. 26.

См. «Просмотр списка изолированных объектов» на стр. 28.

Исправление и восстановление изолированных файлов

При восстановлении файла попытки уничтожить вирус не предпринимаются. Используйте эту возможность с осторожностью, поскольку существует опасность заражения системы. Например, восстановите файл, если центр Symantec Security Response уведомил вас о том, что файл не заражен. Восстановление потенциально зараженного файла не является безопасной операцией. Восстановленные файлы копируются в исходные папки, если это возможно. Если нет, пользователю предлагается выбрать папку.

При исправлении файла предпринимается попытка уничтожить вирус. Пользователю предлагается выбрать папку для сохранения исправленного файла. С помощью функции исправления можно проверить работоспособность новых описаний в Центральном изоляторе перед их рассылкой.

Для исправления изолированных файлов выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на одном или нескольких файлах и выберите пункт **Исправить.**

См. «Передача файлов для анализа» на стр. 26.

См. «Просмотр списка изолированных объектов» на стр. 28.

См. «Удаление изолированных файлов» на стр. 29.

Глава 4

Работа в режиме осмотра и доставки через Интернет

Эта глава содержит следующие разделы:

Описание режима осмотра и доставки через Интернет

Функция осмотра и доставки через Интернет входит в состав Digital Immune System – автоматизированной системы отправки образцов, анализа и доставки описаний вирусов, позволяющей оперативно организовывать защиту против новых вирусов, выявленных с помощью эвристических методов.

Digital Immune System копирует файлы, которые могут быть заражены новым вирусом, и отправляет их через Интернет в центр Symantec Security Response. Symantec Security Response автоматически анализирует полученные образцы и, в случае обнаружения нового вируса, создает и возвращает описание этого вируса.

Примечание: Новые описания оформляются в виде обновлений для программных продуктов Symantec и Symantec AntiVirus и немедленно рассылаются всем пользователям, которые сообщили о наличии нового вируса. Впоследствии эти описания рассылаются всем остальным пользователям, чтобы предотвратить распространение нового вируса.

Включение и настройка Центрального изолятора, работающего через Интернет

В состав Центрального изолятора входят два компонента: сервер Изолятора, который можно установить на любом компьютере Windows NT/2000 для хранения образцов зараженных файлов и обмена данными с центром Symantec Security Response, и консоль Изолятора, которая представляет собой модуль MMC и применяется для управления работой Изолятора.

Для того чтобы начать использование Центрального изолятора, выполните следующие действия:

- Подключитесь к серверу Изолятора.
- Настройте сервер Изолятора.
- Настройте клиенты для пересылки файлов на сервер Изолятора.
- Настройте функцию осмотра и доставки через Интернет для передачи образцов в центр Symantec Security Response и получения обновленных описаний.

Примечание: Режим осмотра и доставки (через Интернет или по электронной почте) выбирается во время установки сервера Изолятора. Для изменения выбранного режима необходимо заново установить сервер Изолятора.

См. «Подключение к серверу Изолятора» на стр. 33.

См. «Настройка сервера Изолятора» на стр. 34.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

Подключение к серверу Изолятора

Сервер Изолятора настраивается в качестве центрального хранилища зараженных файлов, которые не удалось исправить на компьютерах-клиентах. После этого можно настроить клиенты на отправку копий файлов, хранящихся в их локальных Изоляторах.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

Для подключения к серверу Изолятора выполните следующие действия:

Можно подключиться к серверу Изолятора, расположенному на локальном компьютере, либо другом компьютере.

Для подключения к серверу Изолятора, расположенному на локальном компьютере, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Подключение к серверу**.
2. В окне диалога «Подключение к серверу Изолятора» введите имя сервера и нажмите кнопку **OK**.

Для подключения к серверу Изолятора, расположенному на другом компьютере, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Подключение к серверу**.
2. В окне диалога «Подключение к серверу Изолятора» введите имя сервера.

3 Введите имя пользователя и пароль для входа на сервер.

4 Если компьютер является частью домена, введите имя домена.

См. «Настройка сервера Изолятора» на стр. 34.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

Настройка сервера Изолятора

Для работы Центрального изолятора в режиме осмотра и доставки через Интернет необходимо задать следующую информацию:

- Путь к папке для хранения файлов на сервере Изолятора
- Применяемые сетевые протоколы и порты, через которые передаются данные

Примечание: На основании информации, заданной во время установки, параметрам Центрального изолятора присваиваются значения по умолчанию, которые сами по себе обеспечивают адекватный уровень защиты. Изменять эти параметры не нужно.

См. «Свойства Центрального изолятора» на стр. 35.

См. «Подключение к серверу Изолятора» на стр. 33.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

Настройка Изолятора

Сервер Изолятора получает зараженные образцы с компьютеров, на которых работают программы Symantec и Symantec AntiVirus. Сервер Изолятора является центральным хранилищем зараженных файлов, которые не удалось исправить на компьютерах-клиентах.

После завершения настройки сервера Изолятора настройте параметры клиентов для отправки копий файлов, хранящихся в их локальных Изоляторах.

См. «Настройка пересылки файлов через Интернет на клиентах» на стр. 39.

Для настройки сервера Изолятора выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Общие» и введите полный путь к папке Центрального изолятора.
3. Укажите максимальный размер папки Изолятора.
4. Выберите протоколы, используемые в сети, и укажите порт, через который передаются данные.

   Не используйте порт, зарезервированный другим приложением. Как правило, порты с номерами более 1025 свободны.

Свойства Центрального изолятора

В Табл. 4-1 приведено краткое описание параметров конфигурации, предусмотренных в окне диалога «Свойства Центрального изолятора».

Примечание: На основании информации, заданной во время установки, этим параметрам присваиваются значения по умолчанию, которые сами по себе обеспечивают адекватный уровень защиты. Изменять эти параметры не нужно.

Табл. 4-1 Свойства Центрального изолятора

Свойство	Описание
Общие	Основные параметры Изолятора, такие как путь к папке Изолятора, максимальный размер содержимого папки, сетевой протокол для взаимодействия с клиентами и частота автоматического обновления консоли.

Табл. 4-1 Свойства Центрального изолятора

Свойство	Описание
Связь через Интернет	Параметры связи, в том числе имя компьютера шлюза Symantec и параметры защиты. ■ Функция «Безопасная отправка» обеспечивает отправку образцов вирусов в компанию Symantec с помощью протокола Secure Socket Layer (SSL). ■ Функция «Безопасная загрузка» обеспечивает получение обновленных описаний от компании Symantec с помощью протокола SSL. ■ «Шлюз Symantec Immune System» задает шлюз, который обменивается данными с центром Symantec Security Response.
Брандмауэр	Задайте информацию на этой вкладке, если в вашей сети применяется брандмауэр. ■ Поле «Имя брандмауэра» содержит IP-адрес или имя компьютера брандмауэра. ■ Поле «Порт брандмауэра» содержит номер порта, через который брандмауэр обменивается данными. ■ «Имя пользователя» задает имя для подключения к брандмауэру. ■ «Пароль» задает пароль для подключения к брандмауэру.
Обработка образцов	■ Функция автоматической отправки образцов позволяет автоматически помещать образцы в очередь для анализа. ■ Интервал проверки очереди - это частота, с которой Изолятор проверяет наличие новых объектов. ■ Флажок «Удалить личные данные» обеспечивает безопасность за счет удаления из отправляемых образцов данных, которые могут оказаться конфиденциальными. ■ «Интервал опроса состояния» задает частоту, с которой опрашивается шлюз на предмет изменения состояния переданных образцов.

Табл. 4-1 Свойства Центрального изолятора

Свойство	Описание
Обработка описаний	■ «Номер активного ряда» задает порядковый номер набора описаний, установленного на сервере Изолятора. Порядковые номера применяются только продуктами Symantec AntiVirus Corporate Edition. Они последовательно присваиваются наборам сигнатур. Набор сигнатур с большим порядковым номером заменяет набор сигнатур с меньшим порядковым номером. ■ «Интервал для сертифицированных описаний» задает частоту опроса шлюза с целью получения обновленных сертифицированных описаний. Значение указывается в минутах. Значение по умолчанию - трижды в день.
Установка обновлений	■ Функция «Установить на выбранные серверы (сертифицированные описания)» автоматически устанавливает сертифицированные описания на выбранных серверах. Для выбора серверов нажмите кнопку «Выбрать». ■ Функция «Установить на зараженных клиентов (описания, которые еще не сертифицированы)» автоматически устанавливает несертифицированные описания на компьютерах, где был обнаружен вирус. ■ Функция «На серверы зараженных клиентов (описания, которые еще не сертифицированы)» устанавливает несертифицированные описания на родительский сервер зараженного клиента. ■ Функция «Установить на выбранные серверы (описания, которые еще не сертифицированы)» автоматически устанавливает несертифицированные описания на выбранных серверах. Для выбора серверов нажмите кнопку «Выбрать». ■ «Интервал повтора» задает частоту, с которой сервер пытается отправить обновленные описания, если компьютеры получателей были отключены. Значение указывается в минутах. ■ В поле «Текущий файл описаний вирусов» указана версия и дата создания файла описаний. Версия задается в следующем формате: ГГММДДn, где n - это буква, задающая выпуск.

Табл. 4-1 Свойства Центрального изолятора

Свойство	Описание
Сведения о клиенте	Содержит информацию о клиенте, заданную во время установки. Вы можете изменить эту информацию. Обратите внимание, что должны быть заполнены все поля.
Оповещения	Общие параметры для настройки системы AMS. Нажмите кнопку «Настроить», чтобы задать механизм оповещения (например, электронное сообщение, сообщение на пейджер, вывод окна сообщения на экран и так далее) для каждого события, вызывающего отправку оповещения. Настройка уведомления ■ Поле «Имя события» позволяет включить или выключить условие отправки оповещения. ■ «Время ожидания (мин)» задает интервал времени в минутах, в течение которого должно соблюдаться условие, для того чтобы было отправлено оповещение. Обратите внимание, что для автономных клиентов или клиентов шлюза и групповых программ, которые не получают обновления описаний автоматически, создается оповещение «Не удалось установить описания на компьютеры получателей». Это оповещение вместе со списком FTP-серверов, с которых можно загрузить описания, автоматически передается на вкладку «Ошибки» зараженного объекта и в журнал Изолятора. Если включены оповещения Send Internet Mail (Отправить электронное сообщение) или Write to Event Log (Записать в журнал событий), то они также будут содержать эту информацию.
Общие ошибки	Список ошибок сервера Изолятора, перечисленных в хронологическом порядке.

Настройка пересылки файлов через Интернет на клиентах

Два типа клиентов Центрального изолятора могут пересылать образцы вирусов на сервер Изолятора:

- Управляемые, например, клиенты и серверы Symantec AntiVirus Corporate Edition, управляемые программой Symantec System Center
- Автономные, например, Symantec AntiVirus для Microsoft Exchange и Symantec AntiVirus для Lotus Notes

Основным различием между этими клиентами является способ доставки обновленных описаний вирусов. В случае доставки по электронной почте обновленные описания присылаются по электронной почте для всех указанных платформ и вручную применяются администратором.

В случае доставки через Интернет обновленные описания автоматически доставляются и устанавливаются на те компьютеры, которые используют один из управляемых программных продуктов. Для автономных продуктов обновленные описания вручную загружаются и устанавливаются администраторами после получения уведомления.

См. «Управляемые и автономные продукты» на стр. 45.

Для настройки пересылки образцов с клиентов выполните следующие действия:

Пересылку файлов на сервер Изолятора можно настроить на управляемых и автономных клиентах.

Для того чтобы настроить управляемые клиенты для пересылки образцов на сервер Изолятора, выполните следующие действия:

1. На правой панели консоли Symantec System Center выберите **Все задачи** > **Symantec AntiVirus** > **Параметры Изолятора**.
2. В окне диалога «Параметры Изолятора» выберите **Включить Изолятор или мастер осмотра и отправки**.
3. Выберите параметр **Разрешить пересылку на сервер Изолятора.**

   Если пересылка включена, то клиенты не могут отправлять файлы из своих Изоляторов напрямую в центр Symantec Security Response.
4. В поле «Имя сервера» введите имя, IP-адрес или SPX-адрес сервера Изолятора.

5 Укажите порт и протокол, выбранные при настройке свойств сервера Изолятора.

6 Выберите операцию, которая должна автоматически выполняться в Изоляторе клиента при появлении новых описаний вирусов.

Для того чтобы настроить автономные клиенты для пересылки файлов на сервер Изолятора, выполните следующие действия:

1 Откройте окно настройки параметров пересылки в Изолятор.

  Обратитесь к документации или к справочной системе конкретной программы.

2 Введите имя сервера или IP-адрес компьютера, на котором работает сервер Изолятора.

3 Укажите порт и протокол, заданные при настройке свойств сервера Изолятора.

См. «Подключение к серверу Изолятора» на стр. 33.

См. «Настройка сервера Изолятора» на стр. 34.

Передача образцов для анализа

Параметры на вкладке «Обработка образцов» указывают, будут ли образцы вирусов автоматически отправляться на шлюз. Если режим автоматической отправки не выбран, то находящиеся в Изоляторе образцы потребуется по отдельности отправлять на шлюз.

Параметры автоматической отправки образцов можно изменить. Как правило, образцы отправляются вручную только при возникновении ошибок во время автоматической отправки, а также для изменения очередности обработки выбранных образцов.

См. «Настройка параметров автоматической отправки образцов» на стр. 40.

См. «Отправка файлов вручную» на стр. 41.

Настройка параметров автоматической отправки образцов

Параметры на вкладке «Обработка образцов» указывают, будут ли образцы вирусов автоматически отправляться на шлюз. Если режим автоматической отправки не выбран, то находящиеся в Изоляторе образцы необходимо отправлять на шлюз каждый по отдельности.

Для обеспечения безопасности можно включить режим удаления личных данных из образца перед его отправкой.

Примечание: Параметры отправки для отдельных объектов можно изменить на вкладке «Действия» выбранного объекта Изолятора.

Для настройки параметров обработки образцов выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства.**
2. В окне «Свойства Центрального изолятора Symantec» откройте вкладку «Обработка образцов» и задайте режим обработки образцов.

Отправка файлов вручную

Подозрительные файлы можно вручную отправить для анализа. Образцы, которые можно исправить с помощью описаний, хранящихся на сервере Изолятора или шлюзе, не передаются в центр Symantec Security Response.

Для отправки образцов вручную должны быть выполнены следующие условия:

- Образец не должен быть выбран для автоматической отправки (атрибут X-Sample-Priority равен 0).
- Образец не должен быть уже отправлен (атрибут X-Date-Submitted равен 0).
- Образец не должен быть уже проанализирован (атрибут X-Date-Finished отсутствует или равен 0).

Для того чтобы отправить файлы вручную, выполните следующие действия:

Перед отправкой файлов вручную необходимо задать приоритет образца.

Для того чтобы вручную задать приоритет образца, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.
3. В окне диалога «Свойства» откройте вкладку «Действия» и задайте приоритет отправки.

Для того чтобы вручную отправить объекты в центр Symantec Security Response, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на одном или нескольких файлах и выберите **Все задачи** > **Поставить в очередь на автоматический анализ**.

См. «Настройка параметров автоматической отправки образцов» на стр. 40.

Управление обновлением описаний

Для управления обновлением описаний вирусов настройте следующие параметры:

- Обработка описаний: Как часто Центральный изолятор опрашивает шлюз Symantec Security Response для получения обновленных сертифицированных описаний
- Установка обновлений: Какие компьютеры будут автоматически получать сертифицированные или несертифицированные описания в случае обнаружения новых вирусов в отправленных образцах

Обновления описаний вирусов для автономных клиентов необходимо загружать вручную.

См. «Настройка обработки описаний» на стр. 43.

См. «Автоматическая установка обновленных описаний» на стр. 43.

См. «Получение обновления описаний вручную» на стр. 44.

См. «Управляемые и автономные продукты» на стр. 45.

Настройка обработки описаний

Параметры обработки описаний определяют периодичность опроса шлюза для загрузки новых сертифицированных описаний. Перед выпуском сертифицированных описаний они проверяются в центре Symantec Security Response.

Для настройки параметров обработки описаний выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
2. В окне диалога «Свойства» откройте вкладку «Обработка описаний» и выберите режим обработки описаний.

См. «Автоматическая установка обновленных описаний» на стр. 43.

См. «Получение обновления описаний вручную» на стр. 44.

См. «Управляемые и автономные продукты» на стр. 45.

Автоматическая установка обновленных описаний

Параметры установки описаний определяют, какие компьютеры автоматически получают обновленные описания в случае обнаружения нового вируса.

Для сертифицированных и несертифицированных описаний можно задать разные параметры. Перед выпуском сертифицированных описаний они проверяются в центре Symantec Security Response. Несертифицированные описания автоматически создаются центром Symantec Security Response при обнаружении нового вируса.

Примечание: Если получены описания для вируса, обнаруженного на компьютере, который не выбран для автоматического получения описаний, то этот компьютер можно вручную поставить в очередь на доставку описаний.

Для настройки параметров установки описаний выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.

2 В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Установка обновлений» и задайте режим установки описаний.

См. «Настройка обработки описаний» на стр. 43.

См. «Получение обновления описаний вручную» на стр. 44.

См. «Управляемые и автономные продукты» на стр. 45.

Получение обновления описаний вручную

Компьютер, не получающий обновления описаний автоматически, можно поставить в очередь на получение новых описаний. Для таких компьютеров образец находится в состоянии «Доступно». Для получения описаний вручную должны быть выполнены следующие условия:

- Образец не должен соответствовать критериям для автоматической доставки описаний (атрибут X-Signatures-Priority равен 0).
- Для образца требуются новые описания (атрибут X-Signatures-Sequence больше 0).
- Образец не должен быть уже исправлен (атрибут X-Date-Finished отсутствует или равен 0).

Для того чтобы вручную добавить компьютер в очередь на доставку описаний, выполните следующие действия:

1 На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.

2 На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.

3 В окне диалога «Свойства» откройте вкладку «Действия» и нажмите кнопку **В очередь на доставку описаний**.

Если для данного образца не требуются новые описания, то кнопка «В очередь на доставку описаний» не будет доступна.

См. «Настройка обработки описаний» на стр. 43.

См. «Автоматическая установка обновленных описаний» на стр. 43.

См. «Управляемые и автономные продукты» на стр. 45.

Управляемые и автономные продукты

Клиенты, пересылающие объекты на сервер Изолятора, делятся на два типа: управляемые, например, клиенты Symantec AntiVirus Corporate Edition, управляемые программой Symantec System Center, и автономные, например, Symantec AntiVirus для Microsoft Exchange и Symantec AntiVirus для Lotus Notes. Основное различие между этими клиентами заключается в способе доставки обновленных описаний, который использует Digital Immune System при обнаружении новых вирусов.

- Для управляемых продуктов описания автоматически создаются и устанавливаются при обнаружении нового вируса.
- Обновление автономных продуктов должно выполняться вручную после создания новых описаний в ответ на появление нового вируса. Для таких продуктов создается оповещение, содержащее список FTP-сайтов, с которых можно загрузить описания.

Примечание: Если автономный продукт установлен на компьютере Windows NT/2000, то установите управляемую версию Symantec AntiVirus Corporate Edition на этом же компьютере. Поскольку оба клиента Центрального изолятора используют общий набор описаний, автономный продукт может пересылать зараженные объекты в Центральный изолятор, а управляемый продукт может получать новые описания.

Автоматизация обновления описаний вирусов для автономных продуктов

Для того чтобы описания вирусов автоматически обновлялись для автономного продукта, установите программу Symantec AntiVirus Corporate Edition на компьютер автономного продукта. Поскольку оба продукта используют общий набор описаний, при обновлении Symantec AntiVirus Corporate Edition будет обновлен и автономный продукт. Дополнительным преимуществом этого способа является то, что он обеспечивает защиту компьютера автономного продукта от вирусных атак.

При появлении описаний для автономных продуктов создается оповещение «Не удалось установить описания на компьютеры получателей». Это оповещение содержит адреса FTP-серверов, с которых можно загрузить описания вирусов.

Описания вирусов для автономных продуктов можно обновить тремя способами:

- Вручную
- С помощью Symantec System Center
- Без помощи Symantec System Center

Обновление описаний вручную

Когда Центральный изолятор получает описания для автономного продукта, создается оповещение «Не удалось установить описания на компьютеры получателей». Это оповещение содержит адреса FTP-серверов, с которых можно загрузить описания вирусов.

Процедура обновления описаний вручную

Для того чтобы вручную обновить описания для автономных продуктов, определите расположение обновленных описаний и настройте оповещение, содержащее адреса FTP-серверов.

Для того чтобы определить расположение обновленных описаний для автономных продуктов, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.
3. На вкладке «Ошибки» окна диалога «Свойства» указаны FTP-серверы, с которых можно загрузить обновленные описания.

Для настройки оповещения, содержащего список FTP-серверов, выполните следующие действия:

1. На консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства.**
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Оповещения» и настройте оповещение Send Internet Mail (Отправить электронное сообщение) или Write to Event Log (Записать в журнал событий) для события «Не удалось установить описания на компьютеры получателей».

   Будет отправлено электронное сообщение или внесена запись в журнал событий NT, соответственно.

Обновление с помощью Symantec System Center

Если в сети применяется программа Symantec System Center, то процедура обновления описаний значительно упрощается. Достаточно указать, что программа Symantec AntiVirus Corporate Edition, установленная на том же компьютере, что и автономный продукт, должна автоматически получать сертифицированные описания.

Для обновления описаний с помощью Symantec System Center выполните следующие действия:

1. Установите программу Symantec AntiVirus Corporate Edition для серверов на том компьютере, на котором работает автономный продукт.
2. На левой панели консоли Symantec System Center щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
3. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Установка обновлений» и выберите **Установить на выбранных серверах**.
4. Нажмите кнопку **Выбрать** и выберите компьютер, на котором установлена программа Symantec AntiVirus Corporate Edition.

Обновление без помощи Symantec System Center

Если программа Symantec System Center не применяется, разрешите обмен данными между программой Symantec AntiVirus Corporate Edition и Центральным изолятором, отредактировав реестр. В качестве меры предосторожности создайте резервную копию реестра перед его изменением.

Процедура обновления описаний без помощи Symantec System Center

Описания можно обновить без помощи программы Symantec System Center.

Кроме того, клиент Symantec AntiVirus Corporate Edition можно настроить на пересылку объектов в Центральный изолятор без помощи Symantec System Center.

Для обновления описаний без помощи Symantec System Center выполните следующие действия:

1 В реестре компьютера, на котором установлен сервер Изолятора, отредактируйте следующий раздел:
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Quarantine\Server\Avis

2 Измените значение параметра definitionBlessedBroadcast на 1.

3 В параметре definitionBlessedTargets укажите имя сервера, на котором установлена программа Symantec AntiVirus Corporate Edition.
Можно указать несколько серверов, перечислив их через запятую.
В качестве идентификатора компьютера можно указать только его имя. Если это имя не удастся преобразовать в адрес компьютера, то обновление не будет выполнено. Например, в некоторых случаях к компьютеру можно обращаться только по IP-адресу или только по IPX-адресу.

4 Увеличьте значение параметра configurationChangeCounter на единицу.
Например, если текущее значение равно 10, то измените его на 11.

Для того чтобы разрешить отправку для Symantec AntiVirus Corporate Edition, выполните следующие действия:

1 В реестре компьютера, на котором установлен продукт Symantec AntiVirus Corporate Edition, отредактируйте следующий раздел:
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\VirusProtect6
\CurrentVersion\Quarantine

2 Измените значение параметра ForwardingEnabled на 1.

3 Укажите в параметре ForwardingPort номер порта, который был задан на странице «Общие» при настройке Центрального изолятора Symantec.
Номер порта нужно указать в десятичном формате.

4 Укажите в параметре ForwardingProtocol одно из следующих значений:
- 0 для применения протокола IP
- 1 для применения протокола IPX

5 Укажите в параметре ForwardingServer одно из следующих значений:
- Имя или IP-адрес компьютера, если применяется протокол IP
- <номер сети>.<адрес узла>, если применяется протокол IPX

Для того чтобы определить расположение обновленных описаний для автономных продуктов, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на зараженном объекте и выберите пункт **Свойства**.
3. Адреса FTP-серверов, с которых можно загрузить обновленные описания, указаны на вкладке «Ошибки» окна диалога «Свойства».

Для настройки оповещения, содержащего список FTP-серверов, выполните следующие действия:

1. На консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Оповещения» и настройте оповещение Send Internet Mail (Отправить электронное сообщение) или Write to Event Log (Записать в журнал событий) для события «Не удалось установить описания на компьютеры получателей».

   Будет отправлено электронное сообщение или внесена запись в Журнал событий NT, соответственно.

См. «Настройка обработки описаний» на стр. 43.

См. «Автоматическая установка обновленных описаний» на стр. 43.

См. «Получение обновления описаний вручную» на стр. 44.

Просмотр сведений о состоянии образца

В ходе обмена данными между сервером Изолятора и шлюзом состояние образца можно определить по выполненным действиям и установленным атрибутам.

См. «Просмотр списка изолированных объектов» на стр. 50.

См. «Описание атрибутов отправки» на стр. 51.

См. «Просмотр выполненных над образцом действий» на стр. 52.

См. «Просмотр ошибок отправки» на стр. 52.

Просмотр списка изолированных объектов

Если компьютеры-клиенты настроены на пересылку зараженных объектов на сервер Изолятора, то файлы добавляются в Центральный изолятор. При этом сохраняется информация, указанная в Табл. 4-2.

Табл. 4-2 Информация об изолированном файле

Свойство	Описание
Имя файла	Имя зараженного объекта
Имя пользователя	Имя владельца зараженного файла
Компьютер	Компьютер, на котором был обнаружен зараженный объект
Проанализирован	Указывает, проанализирован ли образец
Возраст	Время, в течение которого образец находится в Изоляторе
Состояние анализа	Состояние анализа образца
Необходимы описания	Порядковый номер набора описаний, необходимого для уничтожения вируса
Состояние образца	Состояние обработки образца
Вирус	Название обнаруженного вируса
Ошибки в обработке образцов	Ошибка при обработке образца

Просмотр списка изолированных объектов или сведений об отдельном объекте

Вы можете просмотреть список изолированных объектов и подробную информацию о каждом объекте.

Для просмотра списка изолированных объектов выполните следующие действия:

- На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec.**

  Изолированные объекты перечислены на правой панели.

Для получения подробных сведений об изолированном объекте выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.

См. «Описание атрибутов отправки» на стр. 51.

См. «Просмотр выполненных над образцом действий» на стр. 52.

См. «Просмотр ошибок отправки» на стр. 52.

Описание атрибутов отправки

Запросы и ответы, которыми обмениваются клиенты и серверы, содержат различные атрибуты, которые полностью описывают образец и его состояние в системе. Эти атрибуты всегда начинаются с символов X-.

Для просмотра атрибутов образца выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.
3. В окне диалога «Свойства» откройте вкладку «Атрибуты образца» и дважды щелкните на имени атрибута, чтобы просмотреть его описание.

См. «Атрибуты образца» на стр. 63.

См. «Просмотр списка изолированных объектов» на стр. 50.

См. «Просмотр выполненных над образцом действий» на стр. 52.

См. «Просмотр ошибок отправки» на стр. 52.

Просмотр выполненных над образцом действий

По выполненным над образцом действиям можно судить о том, был ли отправлен образец, и в каком состоянии находится доставка описаний вирусов.

При необходимости можно изменить параметры доставки выбранного образца, заданные по умолчанию. Кроме того, можно вручную добавить образец в очередь на отправку в центр Symantec Security Response, а также запросить обновленные описания вирусов для выбранного образца.

Для просмотра действий, выполненных над образцом:

1. На левой панели консоли Центрального изолятора Symantec выберите **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.
3. В окне диалога «Свойства» откройте вкладку «Действия» и просмотрите действия, выполненные над образцом.

См. «Просмотр списка изолированных объектов» на стр. 50.

См. «Просмотр ошибок отправки» на стр. 52.

См. «Компоненты Digital Immune System и Центрального изолятора» на стр. 11.

Просмотр ошибок отправки

Если при отправке образца возникла ошибка, то информация о ней будет сохранена в системе. Просмотрите записи об ошибках, чтобы определить, какое действие требуется выполнить над образцом.

Для просмотра ошибок отправки выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec**.
2. На правой панели щелкните правой кнопкой мыши на имени объекта и выберите пункт **Свойства**.
3. Ошибки отправки указаны на вкладке «Ошибки» окна «Свойства».

См. «Просмотр списка изолированных объектов» на стр. 50.

См. «Описание атрибутов отправки» на стр. 51.

См. «Просмотр выполненных над образцом действий» на стр. 52.

Отправка оповещений

Помимо ведения журнала Изолятора, существует возможность отправки оповещений при возникновении событий Центрального изолятора. Предусмотрены следующие способы отправки оповещений:

- Вывод окна сообщения
- Отправка сообщения на пейджер
- Отправка электронного сообщения
- Рассылка широковещательного сообщения
- Добавление записи в журнал событий NT

Примечание: Для автономных клиентов, которые не получают обновления описаний автоматически, генерируется оповещение « Не удалось установить описания на компьютеры получателей». Это оповещение вместе со списком FTP-серверов, с которых можно загрузить описания, автоматически передается на страницу «Ошибка» зараженного объекта и в журнал Изолятора. Если включены оповещения Send Internet Mail (Отправить электронное сообщение) или Write to Event Log (Записать в журнал событий), то они также будут содержать эту информацию.

См. «Настройка оповещений» на стр. 53.

См. «События, вызывающие отправку оповещений» на стр. 55.

Настройка оповещений

В параметрах оповещений задаются события, при возникновении которых Изолятор отправляет оповещения, а также получатели этих оповещений. Каждое событие, при возникновении которого отправляется оповещение, можно включить или выключить независимо от других событий.

Примечание: Для автономных клиентов, которые не получают обновления описаний автоматически, генерируется оповещение «Не удалось установить описания на компьютеры получателей». Это оповещение вместе со списком FTP-серверов, с которых можно загрузить описания, автоматически передается на страницу «Ошибка» зараженного объекта и в журнал Изолятора. Если включены оповещения Send Internet Mail (Отправить электронное сообщение) или Write to Event Log (Записать в журнал событий), то они также будут содержать эту информацию.

Задайте сервер AMS и укажите, кто является получателем оповещения для каждого события. После настройки параметров получателей можно включить или выключить отдельные события на вкладке «Оповещения».

Настройка отправки оповещений и списка получателей оповещений

Вы можете настроить отправку оповещений и задать список получателей этих оповещений.

Для настройки оповещений выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Оповещения» и настройте отправку оповещений.

Для того чтобы задать получателей оповещений и способ отправки оповещений, выполните следующие действия:

1. На левой панели консоли Центрального изолятора Symantec щелкните правой кнопкой мыши на значке **Центральный изолятор Symantec** и выберите пункт **Свойства**.
2. В окне диалога «Свойства Центрального изолятора Symantec» откройте вкладку «Оповещения» и нажмите кнопку **Настроить**.
3. Выберите событие и нажмите кнопку **Настроить**.
4. Для получения дополнительной информации можно нажать кнопку **Справка** на странице мастера.

См. «События, вызывающие отправку оповещений» на стр. 55.

События, вызывающие отправку оповещений

В таблице 4-3 перечислены события, при возникновении которых отправляются оповещения. Эти оповещения можно отследить с помощью AMS.

Табл. 4-3 События, вызывающие отправку оповещений

Событие	Описание
Не удалось подключиться к шлюзу	Агенту Изолятора не удалось подключиться к шлюзу Digital Immune System.
Ошибка Defcast	Defcast – это служба, которая рассылает новые описания вирусов с сервера Изолятора на компьютеры получателей.
Не удалось установить описания на компьютеры получателей	При рассылке новых описаний вирусов возник сбой. Это сообщение также говорит о том, что имеются описания для автономных клиентов.
Нет доступа к каталогу описаний	Серверу Изолятора не удалось найти каталог описаний вирусов.
Не удалось подключиться к сканеру Изолятора	Образцы невозможно осмотреть в изоляторе, и они не будут отправлены на шлюз.
Работа агента Изолятора остановлена	Изолятор не сможет установить связь с шлюзом.
Ожидание необходимых описаний	Описания еще не получены от шлюза.
Появились новые сертифицированные описания	На сервере Изолятора появились новые сертифицированные описания.
Появились новые несертифицированные описания	В ответ на отправку образца серверу Изолятора были переданы новые несертифицированные описания.
Осталось мало места для каталога Изолятора	Каталог Изолятора почти заполнен.
Максимальный размер Изолятора превышает объем свободного места на диске	Задан максимальный объем каталога Изолятора, превышающий объем свободного дискового пространства.
Образец: не был исправлен	Образец либо не был исправлен, либо исправление не требовалось.

Табл. 4-3 События, вызывающие отправку оповещений

Событие	Описание
Образец: не удается установить описания	Не удалось установить описания. Обычно это связано с повреждением набора описаний.
Образец: ошибка обработки	При обработке образца произошла ошибка.
Образец: требуется содействие службы технической поддержки	Образец не удалось обработать автоматически. Обратитесь в службу технической поддержки за содействием.
Образец: отложен для отправки вручную	Образец находится на сервере Изолятора, но не был отправлен автоматически.
Образец: слишком долго не устанавливаются новые описания	Ожидалось, что будут установлены новые описания (состояние свидетельствует об их рассылке), но этого не произошло.
Образец: слишком долго находится в состоянии «Разосланы»	Новые описания получены от шлюза, но подтверждение того, что они установлены на клиенте, еще не получено Изолятором.
Образец: слишком долго находится в состоянии «Требуются»	Описания еще не получены от шлюза.
Образец: слишком долго находится в состоянии «Освобожден»	Ответ от шлюза еще не получен.
Образец: слишком долго находится в состоянии «Отправлен»	Образец еще не получен шлюзом.
Образец: слишком долго находится в состоянии «Помещен в Изолятор»	Образец еще не осмотрен в Изоляторе.
Образец: новые описания готовы к доставке	Новые описания находятся на сервере Изолятора, но их отправка еще не начата.

См. «Отправка оповещений» на стр. 53.

Приложение A

Справка по обработке образцов

Эта глава содержит следующие разделы:

Сведения об обработке образцов

Система Digital Immune System предоставляет информацию обо всех образцах в системе в режиме реального времени. Эта информация включает в себя сведения о состоянии образца и состоянии анализа этого образца.

Состояние образца

В Табл. A-1 перечислены возможные значения состояния образца, описывающие соответствующий этап обработки образца в системе Digital Immune System.

Табл. A-1 Состояние образца

Состояние	Описание
Внимание	Образец требует вмешательства службы технической поддержки.
Доступно	Новые описания получены для доставки на компьютер, представивший образец.
Рассылка	Новые описания поставлены в очередь для доставки на компьютер, представивший образец.
Разосланы	Новые описания доставлены на компьютер, представивший образец.
Ошибка	Произошла ошибка при обработке.
Отложен	Отправка образца отложена.
Установлены	Новые описания установлены на компьютер, представивший образец.
Требуются	Для этого образца требуются новые описания.
Не установлены	Новые описания не удалось доставить на компьютер, представивший образец.
Помещен в Изолятор	Образец получен Центральным изолятором.
Освобожден	Образец поставлен в очередь на анализ.
Перезапуск	Обработка образца будет начата сначала.

Табл. A-1 Состояние образца

Состояние	Описание
Отправлен	Образец отправлен в центр Symantec Security Response для анализа.
Не требуются	Новые описания для этого образца не требуются.

Состояние анализа

В поле «Состояние анализа» показано состояние анализа образца, переданного системе Digital Immune System. Состояние указывает, в какой части сетевой структуры находится образец, какой этап анализа выполняется в настоящее время или каков результат анализа.

Окончательные состояния

Образцы, обработка которых завершена, находятся в одном из окончательных состояний. Все узлы системы Digital Immune System используют окончательные состояния. После того как образец перешел в окончательное состояние, его состояние уже не может измениться. При переводе образца в окончательное состояние устанавливается атрибут X-Date-Analyzed. Его наличие говорит о том, что значение атрибута X-Analysis-State больше не изменится. Окончательные состояния описаны в таблице Табл. A-2.

Табл. A-2 Окончательные состояния

Состояние	Описание
abort	Передача или анализ образца был прерван из-за внутренней программной ошибки.
attention	Образец требует вмешательства службы технической поддержки.
broken	Образец заражен вирусом, но служба разработки описаний сообщила об ошибке, поэтому файлы описаний для этого вируса отсутствуют.
declined	Образец недопустим и был отклонен.
error	Произошла ошибка при обработке.
infected	Образец заражен вирусом, и его можно исправить с помощью имеющихся файлов описаний.

Табл. A-2 Окончательные состояния

Состояние	Описание
misfired	Образец проанализирован, но вирусы в нем не обнаружены, несмотря на обнаруженное заражение. Заражение было ошибочно обнаружено, поскольку в предыдущих файлах описаний содержится ошибка, исправленная в новых файлах описаний.
nodetect	Образец не был проанализирован, но и не содержит какого-либо подозрительного кода.
norepair	Образец заражен вирусом, и его нельзя исправить с помощью имеющихся файлов описаний. Его следует удалить.
uninfectable	Образец не содержит исполняемого кода, вследствие чего он не может быть заражен вирусами. Возможно, исполняемый код не попал в образец, либо образец содержит только данные, например, изображение или звуковой фрагмент.
uninfected	Образец был проанализирован, но вирусы в нем не обнаружены.
unsubmittable	Образец содержит известное вредоносное программное обеспечение, например, «червь» или «троянский конь». Его следует удалить.
Encrypted	Центральному изолятору не удалось осмотреть образец, так как он зашифрован или защищен паролем. Расшифруйте образец или удалите пароль, а затем снова отправьте образец.
Delete	Файлы созданы вредоносным кодом, либо содержат вредоносный код. Единственное, что можно сделать с этими файлами - удалить их.
Restore	Файлы нельзя исправить. Возможно, файлы были случайно изменены или изменены вирусом, либо содержат поврежденный код вируса. Из-за внесенных изменений невозможно исправить файлы, либо это делать небезопасно. Эти файлы следует восстановить из резервной копии.

Состояния передачи

Образцы, еще не доставленные в центр Symantec Security Response, находятся в одном из состояний передачи. Образцы могут находиться в состоянии передачи только за пределами центра Symantec Security Response. Образец может находиться в состоянии ожидания перед переходом в другое состояние сколь угодно долго. Состояния передачи описаны в Табл. A-3.

Табл. A-3 Состояния передачи

Состояние	Описание
accepted	Образец принят шлюзом, но еще не импортирован в центр Symantec Security Response.
importing	Образец импортируется в центр Symantec Security Response.
receiving	Идет прием образца на шлюзе.

Состояния ожидания

Образцы, ожидающие анализа в центре Symantec Security Response, находятся в одном из состояний ожидания. Образцы могут находится в состоянии ожидания только внутри центра Symantec Security Response. Время пребывания в состоянии ожидания перед переходом в другое состояние не ограничено. Состояния ожидания описаны в Табл. A-4.

Табл. A-4 Состояния ожидания

Состояние	Описание
defer	Образец не удалось проанализировать автоматически, и он будет передан специалистам.
deferred	Образец не удалось проанализировать автоматически, и он был передан специалистам.
deferring	Образец не удалось проанализировать автоматически, и он передается специалистам.
imported	Образец импортирован в центр Symantec Security Response, но его анализ еще не начат.
rescan	Образец должен быть повторно осмотрен, так как в центре Symantec Security Response появились новые файлы описаний вирусов.

Активные состояния

В процессе анализа в центре Symantec Security Response образцы находятся в одном из активных состояний. Активные состояния используются только компонентом обработки данных центра Symantec Security Response. Образец может находиться в активном состоянии от нескольких секунд до десятков минут. Активные состояния описаны в Табл. A-5.

Табл. A-5 Активные состояния

Состояние	Описание
archive	Образец ожидает архивации файлов автоматического анализа.
archiving	Идет архивация файлов автоматического анализа.
binary	Образец отнесен к двоичным программам и ожидает обработки двоичным контроллером.
binaryControlling	Двоичный контроллер определяет начальные условия для двоичной репликации.
binaryReplicating	Идет обработка образца модулем двоичной репликации.
binaryScoring	Образец заразил другие двоичные программы, и модуль двоичных расчетов выбирает сигнатуры для обнаружения и удаления вируса.
binaryWait	Образец ожидает освобождения модуля двоичной репликации.
classifying	Идет определение типа данных образца.
fullBuilding	Идет сборка нового набора описаний вирусов с добавлением сигнатур, отобранных для нового вируса.
fullUnitTesting	Идет проверка целостности полного набора файлов описаний.
incrBuilding	Отобранные для нового вируса сигнатуры добавляются в текущие файлы описаний вирусов.
incrUnitTesting	Идет проверка целостности дополненных файлов описаний вирусов.
locking	Получен исключительный доступ к службе создания описаний.

Табл. A-5 Активные состояния

Состояние	Описание
macro	Образец отнесен к документам или электронным таблицам, содержащим исполняемые макросы, и ожидает обработки контроллером макросов.
macroControlling	Контроллер макросов определяет начальные условия для репликации макросов.
macroReplicating	Идет обработка образца модулем репликации макросов.
macroScoring	Образец заразил другие документы или электронные таблицы, и модуль расчетов макросов выбирает сигнатуры для обнаружения и удаления вируса.
macroWait	Образец ожидает освобождения модуля репликации макросов.
сигнатуры	Образец заражен новым вирусом, сигнатуры для его обнаружения и уничтожения выбраны, ожидается выполнение сборки описаний для образца.
unlocking	Освобождается служба создания описаний.

Атрибуты образца

Сообщения с запросами и ответами, которыми обмениваются клиенты и серверы, содержат в заголовках различные атрибуты. Они полностью описывают образец и его состояние в системе Digital Immune System.

Эти атрибуты имеют значение только для клиентов и серверов системы Digital Immune System. Их имена всегда начинаются с символов X-.

Более подробные сведения об отдельных атрибутах приведены в следующих разделах:

- См. «Атрибуты X-Analysis» на стр. 64.
- См. «Атрибут X-Checksum-Method» на стр. 66.
- См. «Атрибуты X-Content» на стр. 66.
- См. «Атрибуты X-Customer» на стр. 68.
- См. «Атрибуты X-Date» на стр. 70.
- См. «Атрибут X-Error» на стр. 73.
- См. «Атрибуты X-Platform» на стр. 74.

- См. «Атрибуты X-Sample» на стр. 79.
- См. «Атрибуты X-Scan» на стр. 85.
- См. «Атрибуты X-Signatures» на стр. 87.

Атрибуты X-Analysis

Атрибуты X-Analysis указываются в сообщениях, передаваемых из центра Symantec Security Response на шлюзы и от шлюзов пользователям, соответственно. Эти атрибуты описывают текущее состояние образца, представленного на анализ.

- См. «X-Analysis-Cookie» на стр. 64.
- См. «X-Analysis-Issue» на стр. 64.
- См. «X-Analysis-Service» на стр. 65.
- См. «X-Analysis-State» на стр. 65.
- См. «X-Analysis-Virus-Identifier» на стр. 65.
- См. «X-Analysis-Virus-Name» на стр. 66.

X-Analysis-Cookie

Этот атрибут содержит изменяющуюся строку, присваиваемую сервером при получении образца. Значение не имеет какого-либо определенного формата и никак не может быть расшифровано клиентами. Клиенты сохраняют значение, возвращенное сервером в ответ на запрос, и используют это значение в качестве аргумента при отправке последующих запросов тому же серверу.

Например, шлюз может назначить образцу такое значение cookie:

- X-Analysis-Cookie: 00000123

X-Analysis-Issue

Этот атрибут содержит изменяющуюся строку, присваиваемую центром Symantec Security Response при получении образца для отслеживания запроса. Значение не имеет какого-либо определенного формата и никак не может быть расшифровано клиентами. Клиенты сохраняют значение, присвоенное центром Symantec Security Response, если оно включено в отчет о состоянии, и позволяют просмотреть это значение пользователю, чтобы он мог ссылаться на него при обращении в службу технической поддержки.

Например, центр Symantec Security Response может присвоить образцу следующий учетный номер:

- X-Analysis-Issue: 00000042

X-Analysis-Service

Этот атрибут указывает, от какого специального класса аналитической службы получены результаты, содержащиеся в сообщении о состоянии образца. Поддерживается только значение quickcheck, которое указывается для частично проанализированных образцов.

Оно означает, что образец не был полностью проанализирован, и получены неопределенные результаты.

Например, сообщение об окончательном состоянии образца, который вероятнее всего не заражен вирусами, но про который нельзя сказать, что он точно не содержит вирусов, может содержать такой заголовок:

- X-Analysis-Service: quickcheck

X-Analysis-State

Этот атрибут содержит текстовый маркер, описывающий текущее состояние анализа образца. Например, образец, который в настоящее время передается из шлюза в центр Symantec Security Response, может находиться в следующем состоянии:

- X-Analysis-State: importing

Успешно реплицированный образец, который готов к операции разделения кода и данных, может находиться в таком состоянии:

- X-Analysis-State: replicated

Отметим, что значение состояния нельзя однозначно определить как окончательное или промежуточное. О том, что образец перешел в окончательное состояние, говорит не значение атрибута X-Analysis-State, а наличие в отчете атрибута X-Date-Finished.

X-Analysis-Virus-Identifier

Этот атрибут содержит цифровой идентификатор обнаруженного в образце вируса.

Например, ниже приведен идентификатор необычного вируса:

- X-Analysis-Virus-Identifier: 32767

X-Analysis-Virus-Name

Этот атрибут содержит текстовую строку с именем обнаруженного в образце вируса.

Например, ниже приведено имя необычного вируса:

- X-Analysis-Virus-Name: Morton.42

Атрибут X-Checksum-Method

Атрибут X-Checksum-Method указывается во всех непустых сообщениях. Этот атрибут сообщает получателю, какой метод использовался для расчета контрольных сумм содержимого. Значением атрибута является название метода. В системе Digital Immune System используется только один метод расчета контрольных сумм — алгоритм Message Digest версии 5 (MD5), описанный в RFC 1321.

Например, если сообщение содержит образец, то в сообщение включается следующий атрибут:

- X-Checksum-Method: md5

Этот атрибут опускается, если сообщение не содержит данных.

Атрибуты X-Content

Атрибуты X-Content соответствующим образом включаются во все непустые сообщения. Эти атрибуты сообщают получателю о том, какие методы использовались для сжатия, шифрования и кодирования содержимого сообщения, если такие методы применялись:

- X-Content-Checksum: Контрольная сумма содержимого, вычисленная по методу MD5
- X-Content-Compression: Метод, использованный для сжатия содержимого
- X-Content-Encoding: Метод, использованный для кодирования содержимого
- X-Content-Scrambling: Метод, использованный для шифрования содержимого

В сообщениях с пустым содержимым эти атрибуты не указываются.

X-Content-Checksum

Этот атрибут содержит контрольную сумму MD5 содержимого, полученного после сжатия, шифрования или кодирования.

Например, контрольная сумма содержимого сообщения может быть такой:

- X-Content-Checksum: 663E6092463AA20EF6A14E8B137AEF30

Этот атрибут используется для проверки правильности содержимого после его передачи.

X-Content-Compression

Этот атрибут задает метод, использованный для сжатия данных, если сжатие применялось. Значением атрибута является название метода сжатия. Система Digital Immune System использует алгоритмы сжатия, описанные группой Info-ZIP.

Табл. A-6 Методы сжатия

Значение	Описание
deflate	Для скопированных образцов
zip	Для каталогов файлов анализа образцов
zip	Для каталогов файлов описаний вирусов

Например, запросы на передачу образца могут содержать следующий атрибут:

- X-Content-Compression: deflate

Этот атрибут опускается, если сообщение не сжималось.

X-Content-Encoding

Этот атрибут задает метод, использованный для кодирования данных, если кодирование применялось. Значением атрибута является название метода кодирования. Единственный метод, применяемый в системе Digital Immune System — алгоритм Base64, описанный в стандарте Multipurpose Internet Mail Extensions (MIME).

Например, если содержимое сообщения закодировано по алгоритму Base64, то это сообщение будет содержать следующий атрибут:

- X-Content-Encoding: base64

Этот атрибут опускается, если сообщение не закодировано.

X-Content-Scrambling

Этот атрибут задает метод, использованный для шифрования данных, если шифрование применялось. Отметим, что содержимое шифруется только для предотвращения случайного запуска потенциально зараженных образцов. Шифрование не обеспечивает защиту данных. Значением атрибута является название метода шифрования. Система Digital Immune System использует единственный метод шифрования — XOR («исключающее или») с постоянной маской.

Например, если содержимое сообщения зашифровано, то это сообщение будет содержать следующий атрибут:

- X-Content-Scrambling: xor-vampish

Этот атрибут опускается, если сообщение не зашифровано.

Атрибуты X-Customer

Атрибуты X-Customer включаются во все сообщения, которые пользователи отправляют на шлюз. Указанные в них сведения служат для идентификации пользователя, отправившего запрос, а также для проверки его полномочий и регистрации. Указанные имена, номера телефонов и электронные адреса в случае необходимости могут применяться сотрудниками службы технической поддержки для обращения к пользователю, отправившему образец.

- X-Customer-Contact-Email: Электронный адрес пользователя
- X-Customer-Contact-Name: Имя пользователя
- X-Customer-Contact-Telephone: Контактный номер телефона пользователя
- X-Customer-Credentials: Регистрационные данные пользователя
- X-Customer-Name: Зарегистрированное имя пользователя
- X-Customer-Identifier: Класс обслуживания пользователя и его идентификатор

X-Customer-Contact-Email

Этот атрибут содержит контактную информацию, применяемую для обращения к пользователю. Значением атрибута является текстовая строка длиной до 255 символов, содержащая электронный адрес, по которому сотрудник службы технической поддержки при необходимости может обратиться к пользователю, отправившему образец.

Ниже приведет пример контактной информации:

- X-Customer-Contact-Email: someone@symantec.com

X-Customer-Contact-Name

Этот атрибут содержит контактную информацию, применяемую для обращения к пользователю. Значением атрибута является текстовая строка длиной до 255 символов, содержащая полное имя пользователя, к которому при необходимости может обратиться сотрудник службы технической поддержки.

Ниже приведет пример контактной информации:

- X-Customer-Contact-Name: Jim Hill

X-Customer-Contact-Telephone

Этот атрибут содержит контактную информацию, применяемую для обращения к пользователю. Значением атрибута является текстовая строка длиной до 255 символов, содержащая номер телефона пользователя, к которому при необходимости может обратиться сотрудник службы технической поддержки.

Ниже приведет пример контактной информации:

- X-Customer-Contact-Telephone: 310-555-1212

X-Customer-Credentials

Этот атрибут используется для передачи регистрационных данных пользователя на шлюз. Значение атрибута применяется шлюзом при получении образца.

Ниже приведен пример регистрационных данных пользователя:

- X-Customer-Credentials: 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

X-Customer-Name

Этот атрибут задает зарегистрированное имя пользователя. Его значением является текстовая строка длиной до 255 символов, задающая имя пользователя и название организации, которая приобрела программный продукт или подписалась на обслуживание.

Ниже приведен пример зарегистрированного имени пользователя:

- X-Customer-Name: Jim Hill, Symantec Corp

X-Customer-Identifier

Этот атрибут содержит данные о классе обслуживания пользователя и его идентификационный номер. Значением атрибута является текстовая строка длиной до 63 символов.

Значение присваивается при установке продукта или при подписке на сетевое обслуживание.

Класс обслуживания обозначается одним из текстовых маркеров, указанных в таблице А-7.

Табл. А-7 Классы обслуживания

Класс	Описание
gold	Для плана обслуживания «gold»
platinum	Для плана обслуживания «platinum»

Например, может быть указан такой идентификатор автора запроса:

- X-Customer-Identifier: 123456-ABCDEFgold 0123456789ABCDEFGHIJ

Атрибуты X-Date

Атрибуты X-Date включаются соответствующим образом во все сообщения. В них содержится дата и время возникновения важных событий в ходе обработки образца или сигнатуры. Ниже перечислены некоторые из сохраняемых значений:

- X-Date-Accessed: Дата и время последнего обращения к файлу
- X-Date-Analyzed: Дата и время анализа образца
- X-Date-Blessed: Дата и время проверки сигнатур
- X-Date-Captured: Дата и время копирования образца
- X-Date-Created: Дата и время создания файла
- X-Date-Distributed: Запланированные дата и время доставки сигнатур
- X-Date-Finished: Дата и время завершения анализа образца
- X-Date-Forwarded: Дата и время помещения образца в Изолятор
- X-Date-Installed: Дата и время установки сигнатур
- X-Date-Modified: Дата и время изменения файла

- X-Date-Produced: Дата и время создания сигнатур в аналитическом центре
- X-Date-Published: Дата и время публикации сигнатур в Интернете
- X-Date-Submitted: Дата и время отправки образцов для анализа

Значение атрибута содержит дату и время возникновения события, зарегистрированное по системным часам отправителя, но приведенное к времени по Гринвичу (GMT) в формате, определенном в RFC 1945 и RFC 822.

Ниже приведен пример значения этого атрибута для данного документа:

- X-Date-Created: Tue, 27 Jan 2000 14:32:45 GMT

При получении сообщения вычисляется разница между показаниями часов отправителя и получателя. Для этого значение атрибута Date сравнивается с показаниями локальных часов. В результате все временные отметки сохраняются по локальным часам.

X-Date-Accessed

Этот атрибут включается в сообщение, если оно содержит образец или набор сигнатур. Значение атрибута задает дату и время последнего обращения к содержащемуся в сообщении файлу.

X-Date-Analyzed

Этот атрибут указывается в сообщении о состоянии образца. Значением атрибута являются дата и время анализа образца.

X-Date-Blessed

Этот атрибут включается в сообщение, если оно ссылается на набор проверенных сигнатур. Значением атрибута являются дата и время публикации этих сигнатур в Интернете. Если этот атрибут указан в сообщении, значит сигнатуры были полностью проверены и заменяют собой все предыдущие сигнатуры.

X-Date-Captured

Этот атрибут включается в сообщение, если оно содержит образец. Значением атрибута являются дата и время первоначального копирования образца.

X-Date-Created

Этот атрибут включается в сообщение, если оно содержит образец или набор сигнатур. Значение атрибута задает дату и время создания содержащегося в сообщении файла.

X-Date-Distributed

Этот атрибут включается в сообщение, если оно ссылается на набор сигнатур, который был поставлен в очередь для доставки на зараженную рабочую станцию. Значением атрибута являются дата и время запланированной доставки.

X-Date-Finished

Этот атрибут указывается в сообщении о состоянии образца. Значением атрибута являются дата и время завершения анализа образца. Если этот атрибут включен в сообщение, значит все атрибуты состояния являются окончательными.

X-Date-Forwarded

Этот атрибут включается в сообщение, если оно ссылается на образец, который был передан в Изолятор. Значением атрибута являются дата и время передачи образца в Изолятор.

X-Date-Installed

Этот атрибут включается в сообщение, если оно ссылается на набор сигнатур, который был установлен на зараженную рабочую станцию. Значением атрибута являются дата и время установки сигнатур.

X-Date-Modified

Этот атрибут включается в сообщение, если оно содержит образец или набор сигнатур. Значение атрибута задает дату и время изменения содержащегося в сообщении файла.

X-Date-Produced

Этот атрибут включается в сообщение, если оно содержит набор сигнатур. Значением атрибута являются дата и время создания этих сигнатур в аналитическом центре.

X-Date-Published

Этот атрибут включается в сообщение, если оно содержит набор сигнатур. Значением атрибута являются дата и время публикации этих сигнатур в Интернете.

X-Date-Submitted

Этот атрибут включается в сообщение, если оно ссылается на образец, который был отправлен на анализ. Значением атрибута являются дата и время отправки образца на Интернет-шлюз.

Атрибут X-Error

Атрибут X-Error указывается в ответных сообщениях, если запросы не удалось правильно обработать. Он описывает причину, по которой не удалось обработать запрос, а также может содержать параметры, более точно описывающие ошибку.

X-Error: код ошибки и дополнительные параметры

Например, сервер, который не может обработать запрос на загрузку набора сигнатур с именем «12345», поскольку эти сигнатуры уже недоступны, может включить в ответное сообщение такой заголовок:

- X-Error: superseded

Сервер, который не может обработать запрос на передачу образца, поскольку значение заголовка «Content-Length» не соответствует размеру содержимого сообщения, может включить в ответ следующий заголовок:

- X-Error: overrun 10138 10139

В Табл. A-8 приведен список кодов ошибок.

Табл. A-8 Коды ошибок

Код	Описание
abandoned	Порядковый номер сигнатуры был отклонен. Обычно эта ошибка связана с тем, что соответствующий набор описаний не прошел проверку целостности.
content	Контрольная сумма содержимого образца не соответствует текущему содержимому.
crumbled	Шлюз не назначил образцу соответствующее значение «cookie».
declined	Образец, отправленный на анализ, не был принят шлюзом. Это может быть связано с тем, что был задан неверный идентификационный номер подписчика. Пользователю следует обратиться в службу технической поддержки.
internal	При обработке образца произошел внутренний сбой.
lost	Образец не был получен полностью из-за сбоя сети.

Табл. A-8 Коды ошибок

Код	Описание
malformed	Один из ключевых атрибутов образца задан в неверном формате.
missing	Один из ключевых атрибутов образца отсутствует.
overrun	Размер содержимого образца превышает указанное значение. Эта ошибка может произойти в результате сетевого сбоя при передаче сообщения.
sample	Контрольная сумма образца не соответствует его содержимому.
superseded	Сигнатура с указанным порядковым номером была заменена на новый сертифицированный набор описаний, и поэтому больше не доступна на сервере. Вместо замещенного набора описаний пользователю рекомендуется загрузить текущий сертифицированный набор описаний.
type	Образец данного типа не поддерживается.
unavailable	Сигнатура с указанным порядковым номером еще не опубликована.
underrun	Фактический размер образца меньше ожидаемого значения.
unpackage	Не удалось распаковать образец или сигнатуру.
unpublished	Не удалось опубликовать набор сигнатур.

Атрибуты X-Platform

Атрибуты X-Platform указываются во всех сообщениях, содержащих образцы. Они описывают аппаратное и программное обеспечение компьютера, скопировавшего образец.

- X-Platform-Address: Список IP- или IPX-адресов
- X-Platform-Correlator: Уникальный коррелятор
- X-Platform-Distributor: Сетевое имя сервера рассылки
- X-Platform-Domain: Имя административного домена
- X-Platform-GUID: Уникальный идентификатор для управляемых компьютеров-клиентов
- X-Platform-Host: Сетевое имя компьютера

- X-Platform-Language: Язык интерфейса операционной системы
- X-Platform-Owner: Зарегистрированный владелец и организация
- X-Platform-Processor: Название производителя, модели и тактовой частоты процессора
- X-Platform-QServer-CountryCode: Код страны компьютера сервера Изолятора по классификации IBM
- X-Platform-QServer-WinINet: Версия Wininet.dll
- X-Platform-QServer-WinINet-Encryption: Уровень шифрования, поддерживаемый текущей версией WinINet
- X-Platform-Scanner: Производитель, название и версия антивирусного продукта
- X-Platform-System: Производитель и версия операционной системы
- X-Platform-User: Сетевое имя пользователя, зарегистрированного в системе

X-Platform-Address

Этот атрибут содержит IP-адрес и IPX-адрес компьютера, скопировавшего образец. Значением атрибута является список IP-адресов и IPX-адресов, представленных в числовом формате и перечисленных через пробел.

Например, адрес компьютера автора этого руководства выглядит так:

- X-Platform-Address: 9.2.18.13

Если компьютер имеет несколько IP-адресов и (или) несколько адресов NetBIOS, все эти адреса включаются в значение атрибута. Такая ситуация является обычной для серверов.

X-Platform-Correlator

Этот атрибут указывает значение, которое присваивается всем образцам, отправленным с конкретной платформы. Значением атрибута является текстовая строка длиной до 32 байт.

Значение атрибута может быть произвольным и не несет смысловой нагрузки, однако должно быть уникальным для каждой платформы. Это значение используется для обозначения образцов, передаваемых с одной и той же платформы, чтобы ограничить количество передаваемых одной платформой образцов. Оно не применяется для идентификации платформы или пользователя.

Например, коррелятор, присвоенный компьютеру автора этого руководства, выглядит так:

- X-Platform-Correlator: 0123456789ABCDEF0123456789ABCDEF

X-Platform-Distributor

Этот атрибут указывает сетевое имя сервера рассылки, с которого компьютеры получают обновления сигнатур. Значением атрибута является строка, содержащая сетевое имя компьютера, на котором работает служба рассылки.

Например, для службы рассылки рабочей станции может быть указано следующее значение:

- X-Platform-Distributor: AVFILES

Этот атрибут не указывается, если административный домен отсутствует.

X-Platform-Domain

Этот атрибут задает административный домен компьютера, скопировавшего образец. Значением атрибута является строка, задающая административный домен LANDesk, к которому относится компьютер, скопировавший образец.

Например, административный домен может быть задан следующим образом:

- X-Platform-Domain: AVBUILD

Этот атрибут не указывается, если административный домен отсутствует.

X-Platform-GUID

Этот атрибут содержит уникальный идентификатор компьютера-клиента, присвоенный программой сетевого управления. Значением атрибута является текстовое представление глобального уникального идентификатора (GUID) без знаков пунктуации.

Например, программа сетевого управления могла присвоить компьютеру-клиенту такой идентификатор:

- X-Platform-GUID: 0123456789ABCDEF0123456789ABCDEF

Этот атрибут не указывается, если компьютер не является управляемым клиентом.

X-Platform-Host

Этот атрибут задает сетевой идентификатор компьютера, скопировавшего образец. Значением атрибута является полное имя TCP/IP или имя NetBIOS.

Ниже приведен пример имени TCP/IP:

- X-Platform-Host: someone.symantec.com

Этот атрибут не указывается, если имя TCP/IP или имя NetBIOS отсутствует.

X-Platform-Language

Этот атрибут указывает язык интерфейса компьютера, скопировавшего образец. Значением атрибута является текстовая строка с названием языка.

Например, если применяется английский язык (США), то будет указано следующее значение:

- X-Platform-Language: English (United States)

X-Platform-Owner

Этот атрибут задает владельца компьютера, скопировавшего образец. Значением атрибута является строка с именем владельца и названием организации.

Например, имя владельца для компьютера автора этого документа, записанное в разделе реестра SOFTWARE\Microsoft\WindowsNT\CurrentVersion, может выглядеть так:

- X-Platform-Owner: Jim Hill, Symantec Corp

X-Platform-Processor

Этот атрибут описывает процессор компьютера, скопировавшего образец. Значением атрибута является строка, содержащая название производителя, модель и тактовую частоту процессора.

Например, в атрибуте могут быть заданы следующие характеристики процессора, содержащиеся в разделе реестра HARDWARE\DESCRIPTION\System\CentralProcessor\0:

- X-Platform-Processor: GenuineIntel 165 MHz x86 Family 5 Model 2 Stepping 12

X-Platform-QServer-CountryCode

Этот атрибут задает код страны компьютера, на котором работает сервер Изолятора, в соответствии с классификацией IBM. Код страны, который также называется кодом страны или региона IBM, основан на международном телефонном коде.

Например, в качестве кода страны может быть задано следующее значение:

- X-Platform-QServer-CountryCode: 1

X-Platform-QServer-WinINet

Этот атрибут задает версию программы WinINet, установленную на сервере Изолятора.

Например, установленная версия WinINet может быть задана следующим образом:

- X-Platform-QServer-WinINet: 5.00.2614.3400

X-Platform-QServer-WinINet-Encryption

Этот атрибут задает уровень шифрования, поддерживаемый программой Internet Explorer, которая установлена на том же компьютере, что и сервер Изолятора. Может поддерживаться 40-разрядное или 128-разрядное шифрование.

Например, уровень шифрования может быть задан следующим образом:

- X-Platform-QServer-WinINet-Encryption:128

X-Platform-Scanner

Этот атрибут описывает средства антивирусной защиты компьютера, скопировавшего образец. Значением атрибута является строка, содержащая название производителя, версию и порядковый номер сигнатур антивирусного продукта.

Например, на компьютере может быть установлена следующая антивирусная защита:

- X-Platform-Scanner: Symantec AntiVirus for Windows version 5.0

X-Platform-System

Этот атрибут описывает операционную систему компьютера, скопировавшего образец. Значением атрибута является строка, содержащая название производителя и версию операционной системы.

Например, название операционной системы компьютера автора этого документа, записанное в разделе реестра SOFTWARE\Microsoft\WindowsNT\CurrentVersion\, выглядит так:

- X-Platform-System: Windows NT 4.0 build 1381 Service Pack 3

X-Platform-User

Этот атрибут задает сетевой идентификатор пользователя, зарегистрированного на компьютере, который скопировал образец. Значением атрибута является строка, содержащая имя пользователя Windows или NetBIOS.

Например, имя пользователя NetBIOS автора этого документа выглядит так:

- X-Platform-User: PRING

Этот атрибут не указывается, если имя Windows и имя NetBIOS отсутствует.

Атрибуты X-Sample

Атрибуты X-Sample включаются во все сообщения, содержащие образцы. Для описания образца применяются следующие атрибуты:

- X-Sample-Changes: Индикатор изменения атрибутов в Изоляторе
- X-Sample-Checksum: Контрольная сумма MD5 для скопированных данных
- X-Sample-Checkup: Запись контрольной базы данных для файлов образцов
- X-Sample-Extension: Расширение для образцов файлов
- X-Sample-File: Диск, каталог и имя образцов файлов
- X-Sample-Geometry: Номер цилиндра, головки и сектора, а также размер сектора
- X-Sample-Priority: Приоритет в очереди
- X-Sample-Reason: Причина копирования образца
- X-Sample-Sector: Адрес на диске для образцов секторов
- X-Sample-Service: Имя запрошенной службы
- X-Sample-Size: Размер скопированных данных
- X-Sample-Status: Состояние образца в Изоляторе

- X-Sample-Strip: Метод, использованный для удаления личных данных пользователя
- X-Sample-Switches: Недокументированные параметры обработки
- X-Sample-Type: Тип образца

X-Sample-Changes

Этот атрибут включается во все сообщения, содержащие образцы. Он указывает на то, что некоторые другие атрибуты образца изменились за время его нахождения в очереди образцов в службе Изолятора. Значением атрибута является целое число, которое увеличивается при добавлении новых атрибутов или изменении значений существующих атрибутов. Само значение не играет никакой роли, но его изменение говорит о том, что в значения других атрибутов были внесены изменения.

Например, после того как образец был скопирован, и агент Изолятора присвоил начальные значения атрибутам, данный атрибут может выглядеть следующим образом:

- X-Sample-Changes: 1

После пересылки образца на сервер Изолятора и добавления к нему нескольких атрибутов, образец может содержать такой атрибут:

- X-Sample-Changes: 2

X-Sample-Checksum

Этот атрибут содержит контрольную сумму MD5 скопированных данных, полученную до сжатия, шифрования или кодирования.

Например, контрольная сумма MD5 образца может выглядеть так:

- X-Sample-Checksum: 8B37247C71443D40A2D7FCF16867803A

Этот атрибут применяется для обнаружения дубликатов и проверки правильности расшифровки и развертывания данных.

X-Sample-Checkup

Этот атрибут включается в сообщения, содержащие образцы. Он содержит запись контрольной базы данных для файла, хранящегося на компьютере, скопировавшего образец. Эта информация, сохраненная еще до заражения образца, полезна для анализа вируса и тестирования инструкций по его устранению.

Например, обычная запись контрольной базы данных может выглядеть так:

- X-Sample-Checkup: 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF012345678

Если на момент копирования образца файла в контрольной базе данных отсутствует запись для этого файла, то данный атрибут не указывается.

X-Sample-Extension

В случае образцов файлов этот атрибут указывает расширение скопированного файла. Атрибут содержит только расширение. Он не включает в себя идентификатор диска, каталог и имя файла, а также точку.

Например, расширение образца файла может выглядеть так:

- X-Sample-Extension: doc

Этот атрибут является избыточным, поскольку расширение файла указывается в атрибуте X-Sample-File. Однако эта избыточность необходима, поскольку атрибут X-Sample-File может быть удален из образца вместе с другими личными данными пользователя перед его отправкой.

X-Sample-File

В случае образцов файлов этот атрибут указывает скопированный файл. Значение содержит идентификатор диска, каталог и имя файла, который был скопирован.

Например, значение этого атрибута может выглядеть следующим образом:

- X-Sample-File: C:\Memos\December.doc

X-Sample-Geometry

Этот атрибут описывает физические параметры диска. Количество цилиндров, головок и секторов указывается в виде трех десятичных значений, разделенных косой чертой, а количество байт в секторе указывается в виде десятичного числа.

Например, параметры диска могут выглядеть следующим образом:

- X-Sample-Geometry: 80/2/18 chs 512 bytes

Формат жесткого диска может выглядеть так:

- X-Sample-Geometry: 800/8/32 chs 512 bytes

X-Sample-Priority

Этот атрибут указывает приоритет образца в очереди. Данное значение определяет важность данного образца по сравнению с другими образцами, находящимися в той же очереди, и порядок обработки образцов в пунктах передачи. Чем больше значение этого атрибута, тем выше приоритет.

Например, приоритет наименее важного образца может быть таким:

- X-Sample-Priority: 1

Приоритет очень важного образца может выглядеть так:

- X-Sample-Priority: 999

X-Sample-Reason

Этот атрибут указывает причину, по которой был скопирован образец. Значением атрибута является текстовый маркер, обозначающий причину копирования образца. Различные варианты причин перечислены в Табл. A-9.

Табл. A-9 Причины копирования образца

Причина	Описание
badrepair	При удалении известного вируса возник сбой
manual	Образец был вручную скопирован пользователем
norepair	Не удалось исправить известный вирус
suspicious	Образец содержит код, похожий на код известного вируса
variant	Образец является новым вариантом известного вируса

Например, образец мог быть скопирован потому, что он заражен новым вирусом, похожим на известный вирус:

- X-Sample-Reason: variant

Другой пример. Образец мог быть скопирован из-за того, что не удалось удалить известный вирус:

- X-Sample-Reason: badrepair

X-Sample-Sector

В случае образцов секторов этот атрибут задает скопированный адрес на диске. Значением атрибута является список адресов секторов. Адреса секторов представляются в виде трех десятичных чисел, разделенных косой

чертой, которые указывают номер цилиндра, номер головки и номер сектора. Скопированные сектора могут быть указаны по отдельности или в виде диапазона. Для диапазона секторов указывается адрес начального сектора и адрес конечного сектора, разделенные дефисом.

Например, для образа всего диска могут быть заданы следующие адреса:

- X-Sample-Sector: 0/0/0-79/1/17

Другой пример. Адреса образца первой дорожки и последнего сектора жесткого диска могут быть заданы следующим образом:

- X-Sample-Sector: 0/0/0-0/0/31 799/7/31

X-Sample-Service

Этот атрибут запрашивает специальный класс службы анализа. Поддерживается только значение quickcheck, которое указывается для тех образцов, которые вряд ли заражены.

Это значение говорит о том, что образец не подлежит полному анализу, который по умолчанию выполняется для обычных образцов. Такие образцы не анализируются полностью, и полученные результаты нельзя считать точными. Атрибут X-Analysis-Service будет указан в сообщении с окончательным состоянием, если полученные результаты не являются точными.

Например, образец, скопированный пользователем вручную, может содержать такой заголовок:

- X-Sample-Service: quickcheck

X-Sample-Size

Этот атрибут задает размер скопированных данных до сжатия, шифрования или кодирования. Значение представляет собой количество байт в десятичном формате.

Например, размер образца большого документа может быть таким:

- X-Sample-Size: 12345678

X-Sample-Status

Этот атрибут указывает состояние образца, пока он находится в очереди образцов службы Изолятора. Значением атрибута является текстовый

маркер, описывающий текущее состояние образца. Возможные состояния образца описаны в Табл. A-10.

Табл. A-10 Состояния образца

Состояние	Описание
available	Доступны новые сигнатуры
distributed	Новые сигнатуры были разосланы получателям
held	Отправка образца отложена
installed	Новые сигнатуры установлены
needed	Требуются новые сигнатуры
released	Образец освобожден для отправки
submitted	Образец отправлен для анализа
unneeded	Новые сигнатуры не требуются

Например, образец, который еще не отправлен на анализ, может находиться в следующем состоянии:

- X-Sample-Status: held

Другой пример. Образец, который был проанализирован и признан зараженным новым вирусом, может находиться в следующем состоянии:

- X-Sample-Status: available

X-Sample-Strip

Этот атрибут указывает метод, использованный для удаления личных данных пользователя из образца. Значением атрибута является название метода удаления. Личные данные пользователя могут быть удалены из образца во время копирования или в любое время после него. После удаления личных данных из образца значения таких атрибутов, как X-Sample-Checksum и X-Sample-Size, соответствуют новому содержимому образца, отправленного на анализ, а не данным исходного файла.

Например, если личные данные были удалены из образца путем их замещения нулями, то сообщение может содержать такой атрибут:

- X-Sample-Strip: overwrite-zeroes

Этот атрибут не указывается, если личные данные не удалялись из образца.

X-Sample-Switches

Этот атрибут задает недокументированные параметры, влияющие на обработку образца в центре Symantec Security Response. В качестве значения атрибута указывается один или несколько маркеров, разделенных пробелами.

X-Sample-Type

Этот атрибут задает тип скопированного образца. Возможные типы описаны в Табл. A-11.

Табл. A-11 Типы образцов

Тип	Описание
file	Образец файла
sector	Образец сектора

Например, тип образца секторов всего диска может быть указан так:

- X-Sample-Type: sector

Атрибуты X-Scan

Атрибуты X-Scan включаются во все сообщения, содержащие образцы. Они описывают результаты проверки образца на наличие известных вирусов с помощью последней версии сигнатур.

- X-Scan-Result: Результат проверки образца
- X-Scan-Signatures-Name: Имя сигнатур, применявшихся для проверки образца
- X-Scan-Signatures-Sequence: Порядковый номер сигнатур, применявшихся для проверки
- X-Scan-Signatures-Version: Номер (дата) версии сигнатур
- X-Scan-Virus-Identifier: Идентификатор обнаруженного вируса
- X-Scan-Virus-Name: Имя обнаруженного вируса

X-Scan-Result

Этот атрибут указывает результаты проверки образца. Возможные результаты перечислены в Табл. A-12.

Табл. A-12 Результаты проверки

Результат	Описание
badrepair	Сбой модуля исправления.
badscan	Сбой модуля осмотра.
completed	Осмотр завершен, но результаты недоступны.
heuristic	Образец может содержать новый вирус.
nodetect	Образец не содержит известных вирусов.
norepair	Вирус, заразивший образец, нельзя удалить имеющимися средствами.
overrun	Модуль исправления записал данные за пределами буфера образца.
repaired	Вирус, заразивший образец, можно удалить имеющимися средствами.
underrun	Модуль исправления записал данные за пределами буфера образца.
unrepairable	Вирус, заразивший образец, нельзя удалить.
unsubmittable	Вероятно, образец является «троянским конем».

Например, если образец мог быть заражен вариантом нового вируса, но подтвердить это не удалось, результат может быть таким:

- X-Scan-Result: heuristic

X-Scan-Signatures-Name

Этот атрибут задает имя сигнатур, применявшихся при проверке образца.

Например, имя полного набора файлов описаний сигнатур вирусов для продуктов Windows 95/98/NT может выглядеть следующим образом:

- X-Scan-Signatures-Name: 00000678.all.zip

X-Scan-Signatures-Sequence

Этот атрибут задает порядковый номер сигнатур, применявшихся при проверке образца.

Например, порядковый номер файлов описаний сигнатур вирусов может выглядеть следующим образом:

- X-Scan-Signatures-Sequence: 00000678

X-Scan-Signatures-Version

Этот атрибут задает версию файлов описаний сигнатур вирусов, применявшихся при проверке файла.

Например:

- X-Scan-Signatures-Version: 1999.02.06.001

X-Scan-Virus-Identifier

Этот атрибут содержит идентификатор обнаруженного в образце вируса.

Например:

- X-Scan-Virus-Identifier: 32767

X-Scan-Virus-Name

Этот атрибут задает имя обнаруженного в образце вируса.

Например:

- X-Scan-Virus-Name: Morton.42

Атрибуты X-Signatures

Атрибуты X-Signatures включаются во все сообщения, содержащие файлы описаний сигнатур вирусов или ссылающиеся на них. Они описывают наборы сигнатур, созданные в аналитическом центре.

- X-Signatures-Checksum: Контрольная сумма MD5 пакета описаний
- X-Signatures-Priority: Приоритет в очереди
- X-Signatures-Sequence: Порядковый номер набора сигнатур
- X-Signatures-Version: Номер (дата) версии набора сигнатур

X-Signatures-Checksum

Этот атрибут задает контрольную сумму пакета файлов описаний сигнатур вирусов, рассчитанную по методу MD5.

Например, контрольная сумма MD5 пакета описаний для всех продуктов может выглядеть так:

- X-Signatures-Checksum: 8B37247C71443D40A2D7FCF16867803A

X-Signatures-Priority

Этот атрибут задает приоритет сигнатур в очереди. Значением атрибута является целое число без знака из диапазона 0-100. Чем больше это значение, тем выше приоритет.

Например, приоритет наименее важных сигнатур может выглядеть следующим образом:

- X-Signatures-Priority: 0

Приоритет более важных сигнатур может быть задан следующим образом:

- X-Signatures-Priority: 1

X-Signatures-Sequence

Этот атрибут задает порядковый номер файлов описаний сигнатур вирусов.

Например, порядковый номер набора может выглядеть следующим образом:

- X-Signatures-Sequence: 00000678

X-Signatures-Version

Этот атрибут задает номер версии файлов описаний сигнатур вирусов.

Например, номер версии набора сигнатур может выглядеть так:

- X-Signatures-Version: 1999.02.06.001

Ошибки в обработке образцов

Возможные ошибки в обработке образцов перечислены в таблице A-13.

Табл. A-13 Ошибки в обработке образцов

Ошибка	Описание
abandoned	Порядковый номер сигнатуры был отклонен. Обычно эта ошибка связана с тем, что соответствующий набор описаний не прошел проверку целостности.
content	Контрольная сумма содержимого образца не соответствует текущему содержимому.
crumbled	Шлюз не назначил образцу соответствующее значение «cookie».
declined	Образец, отправленный на анализ, не был принят шлюзом. Пользователю следует обратиться в службу поддержки.
internal	При обработке образца произошел внутренний сбой.
lost	Образец не был получен полностью из-за сбоя сети.
malformed	Один из ключевых атрибутов образца задан неверно.
missing	Один из ключевых атрибутов образца отсутствует.
overrun	Размер содержимого образца превышает указанное значение. Эта ошибка может произойти в результате сетевого сбоя при передаче сообщения.
sample	Контрольная сумма образца не соответствует его содержимому.
superseded	Сигнатура с указанным порядковым номером была заменена на новый сертифицированный набор описаний, и поэтому больше не доступна на сервере. Вместо замещенного набора описаний пользователю рекомендуется загрузить текущий сертифицированный набор описаний.
type	Образец данного типа не поддерживается.
unavailable	Сигнатура с указанным порядковым номером еще не опубликована.
underrun	Фактический размер образца меньше ожидаемого значения.
unpackage	Не удалось распаковать образец или сигнатуру.
unpublished	Не удалось опубликовать набор сигнатур.

Алфавитный указатель

П

С

Т

У

Ф

Ц

Ш

A

D

H

L

M

S

X

Обслуживание и техническая поддержка

Компания Symantec стремится обеспечивать высокое качество обслуживания клиентов во всем мире. Она предоставляет помощь профессионалов в любой точке мира для решения вопросов, связанных с применением программного обеспечения и услуг.

Порядок обслуживания клиентов и технической поддержки в разных странах различен.

Если у вас возникнут вопросы относительно описанных ниже услуг, обратитесь к разделу «Центры обслуживания клиентов и технической поддержки».

Регистрация и лицензии

Если для работы с продуктом необходима регистрация или код лицензии, рекомендуем вам обратиться на Web-сайт регистрации и лицензирования фирмы Symantec, расположенный по адресу www.symantec.com/certificate. Кроме того, можно обратиться по адресу http://www.symantec.com/techsupp/ent/enterprise.html, выбрать программный продукт, который необходимо зарегистрировать, и воспользоваться соответствующей ссылкой для лицензирования и регистрации на домашней странице этого продукта.

Если вы приобрели подписку на техническую поддержку, то для решения технических вопросов можно обратиться в компанию Symantec по телефону или через Интернет. При первом обращении в службу технической поддержки будьте готовы назвать номер вашего лицензионного сертификата или контактный идентификатор, полученный при регистрации продукта, чтобы сотрудники службы поддержки могли

проверить ваше право на получение соответствующей услуги. Если вы не приобрели подписку на техническую поддержку, то для получения подробных сведений о предоставляемых услугах технической поддержки обратитесь в отдел обслуживания клиентов фирмы Symantec или по месту приобретения продукта.

Обновление средств защиты

Самые последние сведения о вирусах и потенциальных угрозах можно получить на Web-сайте Symantec Security Response (ранее называвшемся Центром антивирусных исследований – Antivirus Research Center) по адресу:

http://securityresponse.symantec.com

На этом сайте представлены обширные сведения по вопросам обеспечения безопасности и о вирусных угрозах, а также новейшие файлы описаний вирусов. Описания вирусов также можно загрузить с помощью функции LiveUpdate, входящей в состав программных продуктов.

Продление подписки на получение антивирусных обновлений

Приобретение вместе с программным продуктом пакета услуг по его обслуживанию позволяет загружать бесплатные обновления описаний вирусов на протяжении срока действия договора об обслуживании. Если срок действия договора об обслуживании закончился, обратитесь по месту приобретения продукта или в отдел обслуживания клиентов компании Symantec за информацией об условиях продления договора об обслуживании.

Web-сайты компании Symantec

Домашняя страница Symantec на различных языках

На английском языке:	http://www.symantec.com
На русском языке:	http://www.symantec.ru
На французском языке:	http://www.symantec.fr
На немецком языке:	http://www.symantec.de
На итальянском языке:	http://www.symantec.it
На голландском языке:	http:// www.symantec.nl

Symantec Security Response

http://securityresponse.symantec.com

Страница Symantec Enterprise Service and Support

http://www.symantec.com/techsupp/bizsolutions/

Бюллетени новостей для отдельных продуктов

США и Азиатско-Тихоокеанский регион, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html.

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Техническая поддержка

Являясь составной частью центра Symantec Security Response, наша группа глобальной технической поддержки обеспечивает работу центров поддержки по всему миру. Нашей основной деятельностью являются ответы на вопросы о функциях и программных продуктах, их установке и настройке, а также пополнение базы знаний, доступной через Интернет. Мы работаем в тесном сотрудничестве с другими подразделениями компании Symantec, что позволяет отвечать на ваши вопросы в кратчайшие сроки. Например, мы сотрудничаем с отделом разработки продуктов и с антивирусными исследовательскими центрами для обеспечения работы служб оповещения и обновления описаний вирусов в случае распространения новых вирусов и для рассылки оповещений. Мы предлагаем следующие услуги:

- Различные варианты поддержки, позволяющие выбрать набор необходимых услуг для организации любого размера;
- Предоставление поддержки по телефону и через Интернет, что позволяет найти решение в кратчайшие сроки и получить самую свежую информацию;
- Обновления программных продуктов, позволяющие автоматически обновлять средства защиты;
- Обновления сигнатур и описаний вирусов, обеспечивающие высокий уровень безопасности;
- Глобальная поддержка с участием специалистов центра Symantec Security Response, доступная ежедневно и круглосуточно по всему миру на нескольких языках;
- Дополнительные функции, такие как служба оповещения Symantec и возможность назначения менеджера по техническим вопросам, расширяющие возможности для получения эффективной и профессиональной поддержки.

Сведения о предлагаемых в настоящее время программах поддержки можно получить на нашем Web-сайте.

Что необходимо для обращения в службу поддержки

Пользователи, заключившие договор о технической поддержке, могут обращаться в службу технической поддержки по телефону или через Интернет по следующему адресу или по адресу одного из указанных ниже Web-сайтов региональной службы поддержки.

www.symantec.com/techsupp/ent/enterprise.html

При обращении в службу поддержки вам потребуется сообщить следующую информацию:

- Номер версии программного продукта
- Сведения об аппаратном обеспечении
- Объем оперативной памяти, емкость диска, сведения о сетевом адаптере
- Сведения об операционной системе
- Номер версии и пакета обновления
- Топология сети
- Сведения о маршрутизаторе, шлюзе и IP-адресах
- Описание возникших неполадок
- Сообщения об ошибках, файлы журналов
- Действия по устранению неполадок, выполненные перед обращением в компанию Symantec
- Сведения об изменениях, недавно внесенных в конфигурацию программного обеспечения или сети

Обслуживание клиентов

В Центре обслуживания клиентов компании Symantec можно получить сведения по вопросам, не связанным с технической поддержкой, например:

- Общие сведения о продукте (например, основные функции, поддерживаемые языки, торговые представительства в вашем регионе и т.д.)
- Основные методы устранения неполадок, например, как узнать версию продукта
- Последние данные об обновлениях программного продукта

- Инструкции по обновлению и модернизации программного продукта
- Инструкции по регистрации программного продукта или лицензии
- Сведения о программах лицензирования компании Symantec
- Информация о контрактах на льготное обновление и обслуживание
- Замена компакт-дисков и руководств
- Обновление регистрационных данных в связи с изменением адреса или имени владельца программного продукта
- Описание различных вариантов технической поддержки, предлагаемых компанией Symantec

Подробные сведения об обслуживании клиентов можно получить на Web-сайте обслуживания и поддержки компании Symantec, а также в центре обслуживания клиентов компании Symantec. Номера телефонов и адреса Web-сайтов центра обслуживания клиентов, расположенного в вашем регионе, можно найти в разделе «Центры обслуживания клиентов и технической поддержки», приведенном в конце главы.

Центры обслуживания клиентов и технической поддержки

Европа, Ближний Восток и Африка

Web-сайты обслуживания и технической поддержки компании Symantec

На английском языке:	www.symantec.com/eusupport/
На французском языке:	www.symantec.fr/frsupport
На немецком языке:	www.symantec.de/desupport/
На итальянском языке:	www.symantec.it/itsupport/
На голландском языке:	www.symantec.nl/nlsupport/
FTP-сайт компании Symantec: (Загрузка сведений по техническим вопросам и последних пакетов обновлений)	ftp.symantec.com

Посетите Web-сайты обслуживания и технической поддержки компании Symantec, на которых можно найти технические и общие сведения о различных программных продуктах.

Symantec Security Response

http://securityresponse.symantec.com

Бюллетени новостей для отдельных продуктов

США, на английском языке:

http://www.symantec.com/techsupp/bulletin/index.html

Европа, Ближний Восток и Африка, на английском языке:

http://www.symantec.com/region/reg_eu/techsupp/bulletin/index.html

На французском языке:

http://www.symantec.com/region/fr/techsupp/bulletin/index.html

На немецком языке:

http://www.symantec.com/region/de/techsupp/bulletin/index.html

На голландском языке:

http://www.symantec.com/region/nl/techsupp/bulletin/index.html

На итальянском языке:

http://www.symantec.com/region/it/techsupp/bulletin/index.html

Отдел обслуживания клиентов компании Symantec

Для получения информации, не касающейся технических вопросов, и рекомендаций по выполнению ряда задач можно обратиться по указанным ниже телефонам на одном из следующих языков: английском, немецком, французском или итальянском:

Австрия	+ (43) 1 50 137 5030
Бельгия	+ (32) 2 2750173
Великобритания	+ (44) 20 7744 0367
Германия	+ (49) 69 6641 0315
Дания	+ (45) 35 44 57 04
Ирландия	+ (353) 1 811 8093
Испания	+ (34) 91 7456467
Италия	+ (39) 02 48270040
Люксембург	+ (352) 29 84 79 50 30
Нидерланды	+ (31) 20 5040698

Норвегия	+ (47) 23 05 33 05
Финляндия	+ (358) 9 22 906003
Франция	+ (33) 1 70 20 00 00
Швеция	+ (46) 8 579 29007
Швейцария	+ (41) 2 23110001
ЮАР	+ (27) 11 797 6639
Прочие страны (только на английском языке)	+ (353) 1 811 8093

Почтовый адрес отдела обслуживания клиентов компании Symantec

Symantec Ltd
Customer Service Centre
Europe, Middle East and Africa (EMEA)
PO Box 5689
Dublin 15
Ireland

Сведения для клиентов из Азиатско-Тихоокеанского региона

Компания Symantec обеспечивает техническую поддержку и обслуживание клиентов по всему миру. В различных странах обслуживание клиентов организовано по-разному. В частности, в некоторых регионах нет представительства компании Symantec, и указанные услуги предоставляются международными партнерами Symantec. Для получения общей информации обратитесь в региональный отдел обслуживания и поддержки компании Symantec.

Отделы обслуживания клиентов и технической поддержки

Австралия

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Australia

Основной номер телефона	+61 2 8879 1000	
Факс	+61 2 8879 1001	
Web-сайт	http://service.symantec.com	
Техническая поддержка по плану Gold	1800 805 834	gold.au@symantec.com
Информация о контрактах технической поддержки	1800 808 089	contractsadmin@symantec.com

Гонконг

Symantec Hong Kong
Central Plaza
Suite #3006
30th Floor, 18 Harbour Road
Wanchai
Hong Kong

Основной номер телефона	+852 2528 6206
Техническая поддержка	+852 2528 6206
Факс	+852 2526 2646
Web-сайт	http://www.symantec.com.hk

Индия

Symantec India
Suite #801
Senteck Centrako
MMTC Building
Bandra Kurla Complex
Bandra (East)
Mumbai 400051, India

Основной номер телефона	+91 22 652 0658
Факс	+91 22 652 0671
Web-сайт	http://www.symantec.com/india
Техническая поддержка:	+91 22 657 0669

Китай

Symantec China
Unit 1-4, Level 11,
Tower E3, The Towers, Oriental Plaza
No.1 East Chang An Ave.,
Dong Cheng District
Beijing 100738
China P.R.C.

Основной номер телефона	+86 10 8518 3338
Техническая поддержка	+86 10 8518 6923
Факс	+86 10 8518 6928
Web-сайт	http://www.symantec.com.cn

Корея

Symantec Korea
15,16th Floor
Dukmyung B/D
170-9 Samsung-Dong
KangNam-Gu
Seoul 135-741
South Korea

Основной номер телефона	+822 3420 8600
Факс	+822 3452 1610
Техническая поддержка	+822 3420 8650
Web-сайт	http://www.symantec.co.kr

Малайзия

Symantec Corporation (Malaysia) Sdn Bhd
31-3A Jalan SS23/15
Taman S.E.A.
47400 Petaling Jaya
Selangor Darul Ehsan
Malaysia

Основной номер телефона	+603 7805 4910
Факс	+603 7804 9280
Электронный адрес для юридических лиц	gold.apac@symantec.com
Номер телефона для бесплатных звонков	1800 805 104
Web-сайт	http://www.symantec.com.my

Новая Зеландия

Symantec New Zealand
Level 5, University of Otago Building
385 Queen Street
Auckland Central 1001
New Zealand

Основной номер телефона	+64 9 375 4100	
Факс	+64 9 375 4101	
Web-сайт службы технической поддержки	http://service.symantec.co.nz	
Техническая поддержка по плану Gold	0800 174 045	gold.nz@symantec.com
Информация о контрактах технической поддержки	0800 445 450	contractsadmin@symantec.com

Сингапур

Symantec Singapore
3 Phillip Street
#17-00 & #19-00 Commerce Point
Singapore 048693

Основной номер телефона	+65 6239 2000
Факс	+65 6239 2001
Техническая поддержка	+65 6239 2099
Web-сайт	http://www.symantec.com.sg

Тайвань

Symantec Taiwan
2F-7, No.188 Sec.5
Nanjing E. Rd.,
105 Taipei
Taiwan

Основной номер телефона	+886 2 8761 5800
Техническая поддержка для организаций	+886 2 8761 5800
Факс	+886 2 2742 2838
Web-сайт	http://www.symantec.com.tw

Мы сделали все возможное, чтобы представленная здесь информация была полной и точной. Тем не менее, содержащаяся в настоящем документе информация может быть изменена безо всякого уведомления. Корпорация Symantec оставляет за собой право на внесение таких изменений без предварительного уведомления.